TOP SECRET

CINE

te urmărește?



adevărul înspăimântător despre Stat, supraveghere și libertate personală

JOHN GIBB

John Gibb

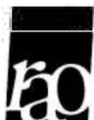
CINE TE URMĂREŞTE?

JOHN GIBB

TOP SECRET

CINE te urmărește?

adevărul
înspăimântător
despre Stat,
supraveghere
libertate personală



rao international publishing company

Descrierea CIP a Bibliotecii Naţionale a României
JOHN GIBB
Cine te urmăreşte? / John Gibb; trad.: Ionuţ Mihai Fulger. -
Bucureşti: RAO International Publishing Company, 2009

ISBN 978-973-54-0069-9

I. Fulger, Ionuţ Mihai (trad.)
821.111-31=135.1

RAO International Publishing Company
Grupul Editorial RAO
Str. Turda nr. 117–119, Bucureşti, România
www.raobooks.com
www.rao.ro

JOHN GIBB
Who's watching you?

Traducere din limba engleză
Ionuţ Mihai Fulger

mai 2009

ISBN 978-973-54-0069-9

Cuprins

Prefață

Pe 11 septembrie 2001, la 8.45 a.m., lumea s-a schimbat – brusc şi definitiv. Acesta a fost momentul în care zborul 11 al American Airlines a intrat în turnul dinspre nord al World Trade Center din New York. După 18 minute, zborul 175 al United Airlines a lovit turnul dinspre sud. Acesta din urmă s-a prăbuşit primul, la 9.58 a.m. Turnul dinspre nord s-a năruit şi el după o jumătate de oră. Pentru Statele Unite ale Americii, aceasta a reprezentat o atrocitate înfiorătoare declanşată – aparent fără avertizare – de către Al Qaeda, pe atunci doar o organizaţie teroristă islamică obscură şi subestimată, care opera din peşterile adânci ale munţilor din Afganistan. Şocate şi silite să reacţioneze, Statele Unite au ripostat, folosindu-şi întreaga forţă militară, pentru a distruge guvernul taliban al Afganistanului, care îi adăpostise pe făptaşi, şi de a scoate Al Qaeda din fortăreţele ei subterane.

Însă, pe lângă acest conflict foarte sângeros, Statele Unite au pornit un război secret împotriva unui duşman invizibil: reţeaua teroristă mondială, alcătuită din membrii şi susţinătorii Al Qaeda. Atacul din 9/11 fusese plănuit cu meticulozitate. Cei 19 bărbaţi care l-au executat erau bine antrenaţi, finanţaţi cu dărnicie şi aveau inestimabilul avantaj de a fi dispuşi să moară pentru cauza lor. Această combinaţie de bani, inteligenţă şi hotărâre punea guvernul american într-un pericol fără precedent, căruia trebuia să îi corespundă o replică intransigentă – cel puţin în ceea ce priveşte libertăţile cetăţeneşti. Statele Unite au răspuns prin înfiinţarea rapidă a Departamentului Securităţii Interne, precum şi prin elaborarea şi intrarea în vigoare a legii „Patriot Act", decizii care – combinate cu spaima provocată de atacul propriu-zis –

au declanşat paranoia şi confuzie în rândul poliţiilor şi agenţiilor de securitate.

Deodată, aceste măsuri au subminat grav multe dintre drepturile şi libertăţile care fuseseră păstrate cu sfinţenie în Constituţia Statelor Unite şi apoi întărite prin nenumărate sentinţe juridice. Administraţia Statelor Unite a investit sume uriaşe în dezvoltarea unor sisteme prin care să poată ţine sub observaţie publicul şi schiţa un profil comportamental pentru orice persoană care ar fi putut fi bănuită că este un „inamic al statului“. Toate acestea au dat naştere unui climat de teamă, în care supravegherea cetăţenilor americani a putut fi sporită, devenind astfel chiar şi mai intensă, dar pe deplin justificabilă pentru un popor american care nu se dezmeticise încă după şocul provocat de atacul Al Qaeda.

Noi, britanicii, am urmărit furtuna izbucnită în Statele Unite şi ne-am reamintit că trecuserăm şi noi prin toate astea, când cu Armata Republicană Irlandeză (IRA). Însă, fără îndoială, în comparaţie cu ambiţiile globale ale Al Qaeda, Irlanda de Nord nu depăşea cu mult proporţiile unei mici încurcături provinciale. În numai câteva luni, am arestat grupuri de extremişti islamici care, din câte se părea, se aflau în Marea Britanie ca să ne ucidă pe toţi în propriile paturi. În 2005, guvernul britanic, în frunte cu premierul Tony Blair, a încercat să transforme ameninţarea reprezentată de terorişti, precum asasinul condamnat Kamel Bourgass, într-o justificare suficientă pentru a introduce noi restricţii, fără precedent, ale libertăţilor cetăţeneşti: detenţie pe termen nedefinit fără să existe nici o acuzaţie, folosirea în justiţie a mărturiilor obţinute sub tortură (chiar dacă în afara ţării), mandate de arestare emise mai degrabă de politicieni decât de judecători şi restricţii ale accesului în clădiri publice, incluzând chiar şi Parlamentul.

Aşadar, ce se petrece? Lumea liberă este cu adevărat ameninţată sau totul face parte dintr-o conspiraţie menită să ne erodeze preţioasa intimitate şi libertăţile personale? Această carte schiţează câteva întrebări şi oferă câteva răspunsuri. Faptul că suntem cu toţii urmăriţi nu poate fi negat. Însă cât de atent? Şi de către cine?

Introducere

E dificil de apreciat impactul unui atac terorist dacă tu însuţi nu ai cunoscut direct unul. În cazul meu, a fost un amestec de farsă şi stinghereală. Singurul element serios a fost faptul că era primul dintr-o lungă serie de atacuri ale republicanilor irlandezi asupra Marii Britanii. Ne-am trezit deodată atacaţi cu bombe făcute din îngrăşământ agricol, îndesate în maşini de către nişte puşti din clasa de mijloc (incompetenţi, însă decişi), unii dintre ei vărsându-şi mânia generată de o moştenire de opresiune şi resentimente cu rădăcinile în Evul Mediu.

8 martie 1973. Ziua a început cu triluri de păsări şi un soare plăcut de primăvară. Apoi, după prânz, o adiere de vânt rece a început să şfichiuiască dinspre vest, unduind suprafaţa Tamisei şi desenând o pătură de nori cenuşii, plutind la înălţime mică deasupra oraşului. Mergeam pe Whitehall Place, îndreptându-mă spre Ministerul Agriculturii. Muncitorii Consiliului Local al Londrei îşi încărcau camionul, după ce curăţaseră ferestrele Clubului Naţional Liberal, aflat pe partea vestică a străzii. Orologiul Big Ben bătea de trei fără un sfert, în timp ce eu mă îndreptam spre Whitehall. Mi-au mai trebuit cinci minute pentru a urca scările din dreptul intrării în minister şi am zăbovit câteva clipe, privind arcada de piatră albă, cu relieful ei sculptat, care întruchipa scoici şi snopi de porumb – opera unor deţinuţi, mi s-a spus cândva, ai închisorii Verne de pe insula Portland.

În jurul orei trei fără zece, a explodat bomba. Una puternică, făcută din vreo 80 de kilograme de îngrăşământ agricol, după cum s-a dovedit ulterior. Se afla într-un pachet plasat sub scaunele unui Hillman Hunter de culoarea bronzului, parcat chiar în spatele clădirii. Maşina fusese furată în Belfast şi adusă la Dublin în urmă cu trei săptămâni. I se schimbaseră plăcuţele de înmatriculare şi apoi fusese transportată cu feribotul de la Dun Laoghaire la Fishguard şi apoi la Londra. Dis-de-dimineaţă, Dolours, fiica unui vechi membru al Armatei Republicane Irlandeze (IRA), Albert Price, un fanatic şi nemilos „provo“ (membru al facţiunii paramilitare IRA), condusese Hillmanul din Dolphin Square la Biroul de Recrutare din Great Scotland Yard, şi îl lăsase acolo. La trei fără şase minute, dispozitivul a fost detonat cu una dintre amorsele de fabricaţie cehoslovacă dintr-un transport de marfă donat de colonelul Ghaddafi, liderul libian, şi adus clandestin în ţară. În total, în acea zi patru maşini-capcană fuseseră abandonate în centrul Londrei de către membri ai IRA. La ora unu, presa primise telefoane de avertisment, în care erau divulgate numerele de înmatriculare şi poziţiile maşinilor-capcană. Poliţia metropolitană, pe vremea aceea deloc iute ca fulgerul, a reuşit să găsească două dintre bombe, iar ofiţeri din echipa pirotehnică de intervenţie le-au dezamorsat. Eu am fost victima celei de-a treia bombe. A patra a explodat după şase minute, în faţă la Old Bailey. Am auzit ecoul unei bufnituri metalice în timp ce zăceam la pământ, holbându-mă la o băltoacă de sânge care se formase în dreapta mea.

Energia exploziei din Great Scotland Yard a fost limitată de un bloc compact de grajduri vechi către nord-est şi comprimată de vehiculele parcate în faţă şi în spate. Suflul şi-a găsit o cale de scăpare pe Whitehall Place, unde a erupt, bubuind ca o furtună sub arcada de deasupra Scotland Place şi aducând cu sine cioburi de sticlă şi bucăţi de metal. Mi s-a spus apoi că vidul

provocat de explozie spărsese toate geamurile din Whitehall Place și că eu fusesem prins de extremitatea sa. După câteva secunde, când am reușit să-mi revin în simțiri, m-am trezit așezat pe la jumătatea scărilor, cu un ciob de sticlă înfipt în mine și cu părul plin de praf și geam pisat. Nu am știut exact ce se întâmplase decât mult mai târziu în acea zi, când am aflat din *London Evening News* că fusesem lovit de prima bombă a campaniei continentale purtate de IRA. Bomba de la Old Bailey, plantată într-un Ford Cortina verde, a rănit 186 de persoane. Un bărbat a murit ulterior, ca urmare a unui atac de cord care, a susținut poliția, fusese provocat de trauma detonării. Cei răspunzători pentru atac au fost arestați de poliție și acuzați de crimă.

Am stat o vreme pe trepte, privindu-i pe polițiști venind în fugă din Charing Cross și grăbindu-se de-a lungul străzii, oprindu-se doar pentru a sparge cu bastoanele geamurile mașinilor parcate și urlând unul la altul, cu voci ascuțite, pline de panică și adrenalină. Cineva le ordonase să se răspândească și să caute obiecte suspecte în mașini. Ofițerii din echipa pirotehnică stăteau împrejur – fie în picioare, fie așezați în mașinile lor Land Rover – și fumau, în așteptarea unor instrucțiuni. Mi se părea că zăcusem pe trepte mult timp, deși știu că nu putuseră fi mai mult de câteva minute, și începea să-mi fie clar că Whitehall se golise. Oamenii fugiseră sau fuseseră evacuați din Parlament și clădirile guvernamentale. Whitehall, Victoria Street, Embankment și podul Westminter erau deodată pustii și tăcute, cu excepția ecourilor alarmelor de pe mașinile poliției, care accelerau către capătul străzii. Se pare că trăiam un sentiment de detașare de totul din jur, atunci când un polițist în uniformă, cu o privire sălbatică, a traversat strada către mine, țipând incoerent. S-a postat alături și mi-a ordonat să mă ridic, astfel încât să mă poată percheziționa. Sergentul său a alergat în sus pe scări, pentru a-l domoli înainte să mă ridice și să mă conducă în clădirea ministerială.

Picioarele îmi tremurau şi mă simţeam de parcă fusesem lovit într-o parte de un boxer profesionist. Holul de la intrare, cu marmură şi mahon, era plin de freamăt, dar nu m-a întâmpinat nimeni, aşa că am luat o ceaşcă cu ceai şi l-am rugat pe sergentul de poliţie care făcea de gardă să-i transmită portarului că venisem la întâlnirea, fixată pentru ora trei, cu ministrul Jim Prior. În acel moment, eu păream singura victimă a atacului. Însă aveam să descopăr în curând că mă înşelam. Când, în cele din urmă, personalul de securitate m-a dus afară, unde aştepta o maşină ministerială, ei şi-au cerut scuze pentru penuria de ambulanţe, deoarece toate vehiculele de intervenţie disponibile fuseseră trimise pentru a se ocupa de răniţii de la Central Criminal Court (Tribunalul Penal Central). I-am cerut şoferului să mă ducă înapoi la *Sunday Express,* unde lucram pe atunci. Fără să-şi ia ochii de la drum, el îmi spuse: „Nu face pe nebunul, băiete. Te duc la spital“.

Era ora patru când am depăşit în viteză piaţa Horse Guards Parade. Regimentul de cavalerie îşi înlocuise deja gardienii călare cu soldaţi severi, purtând armură de corp şi ţinând în mâini arme de asalt. Exista un sentiment de irealitate, ca şi cum lumea noastră familiară se sfârşise şi nimic nu avea să mai fie la fel. Am aflat mai apoi, ascultând ce se vorbea în secţia de urgenţă a spitalului Middlesex, că zece bărbaţi şi femei de origine irlandeză fuseseră arestaţi la aeroportul Heathrow. Marea Britanie fusese „închisă“ şi transformată într-un câmp de luptă, nu mai avea nimic din terenul de joacă pe care îl ştiam. În acea zi se împlineau fix 25 de ani de când George Orwell înmânase editorilor săi manuscrisul romanului *1984*.

Douăzeci de ani mai târziu, pe 24 aprilie 1993, IRA a adus o camionetă plină cu explozivi în City (zona cunoscută şi ca „Square Mile“) şi l-a detonat în Bishopsgate, avariind grav NatWest Tower de pe Old Broad Street, numărul 25, şi închizându-l. Acest colos ostentativ fusese proiectat de Richard Seiffert şi finalizat în 1980,

după ce fuseseră investite în el 72 de milioane de lire sterline. Din fericire pentru cei care lucrau acolo, clădirea era solidă, cu un miez din beton care susţinea cele 42 de etaje. Nimeni nu a fost ucis, însă violenţa şi îndrăzneala atacului au avut un efect profund asupra lumii corporatiste din City. Rezultatul a fost un efort susţinut al instituţiilor financiare din zonă de a-i proteja pe bogaţi de nebuni, investind în cel mai înalt nivel de securitate posibil. Revolta bărbaţilor în costume a fost sprijinită de buzunarele lor încăpătoare, iar răspunsul poliţiei şi al forţelor de securitate a venit imediat. Dacă să-i bombardezi pe politicieni şi pe clienţii puburilor părea acceptabil, un atac în City era cu totul altceva. Nu putea exista nici un fel de toleranţă faţă de teroriştii care periclitează pieţele financiare şi de asigurări, ca să nu mai vorbim de integritatea clădirii Old Bailey, leagănul justiţiei şi cel mai mare tribunal din lumea occidentală.

La câteva zile după atacul de la NatWest, un cerc de beton şi oţel fusese înălţat în jurul zonei Square Mile, iar poliţişti în uniformă opreau şi verificau fiecare maşină ce intra în City. În acelaşi timp, camere de supraveghere au început să răsară pe monoliticele clădiri de birouri, ca nişte mici protuberanţe fixate pe pereţi, la şapte metri înălţime. Unele se mişcau odată cu tine, altele arătau, prin aprinderea unui buton roşu, că înregistrează. O unitate de monitorizare a fost înfiinţată şi echipată pe Wood Street, fiind sub controlul secţiei de poliţie Bishopsgate. În mai puţin de un an, poliţia din City dădea ordin ca sisteme de televiziune cu circuit închis să supravegheze până la ultimul centimetru din străzile şi trotuarele din Square Mile. Nu mai exista nici o curte, nici un garaj sau scuar care să nu poată fi monitorizat sau înregistrat, iar poliţiştii nici măcar nu aveau nevoie să apeleze la Ministerul de Finanţe pentru fondurile necesare. Supravegherea era plătită independent de bănci şi instituţii financiare, iar sistemul era proiectat după cerinţele acestora. Banii nu constituiau o problemă.

Pe la începuturile actelor de violenţă ale IRA, serviciile de securitate din afara Londrei dădeau un răspuns neaşteptat de firav forţelor teroriste, bine finanţate. Informaţiile erau puţine, iar în scurt timp, grupul de „provo“ a devenit imprevizibil şi fără scrupule. În primele zile ale sistemului de supraveghere din City, calitatea videocamerelor şi a casetelor era standard, iar imaginile erau în alb-negru. Nu exista facilitatea de a mări un detaliu sau de a lărgi perspectiva, după cum nu existau nici sunet, nici posibilitatea de a identifica un număr de maşină, nici capacitatea de a recunoaşte şi de a capta trăsăturile faciale ale trecătorilor, nici o arhivă digitală. Erau acoperite parţial activităţile din staţiile de metrou, iar cei care priveau ecranele nu erau foarte pricepuţi la asta. Vizitatorilor centrului de supraveghere li se ofereau proiecţii din videotecă, ce includeau exhibiţionişti care, ca urmare a vreunui pariu, se apucaseră să alerge goi între puburile The Green Man din Victoria Street şi Bishop's Finger din Smithfield. Ofiţerii de poliţie cărora li se dăduse sarcina de a sta în faţa unui şir de ecrane de televizor, aşteptând să se întâmple ceva, au găsit treaba asta dificilă şi plictisitoare, aşa că, după cum era de aşteptat, au folosit echipamentul video pentru a înregistra evenimentele care spărgeau monotonia. Totuşi, instituţiile s-au dedicat securităţii cu hotărâre şi fără compromisuri. Consilierii municipali şi-au scos carnetele de cecuri, poliţiştii au fost puşi la punct, iar bancherii şi asiguratorii au putut dormi liniştiţi, acordând din nou afacerilor întreaga lor atenţie.

Corporaţia s-a lăudat că fiecare centimetru din Square Mile putea fi supravegheat de poliţie. Orice îngrijorare publică pe care această declaraţie ar fi putut-o provoca nu a fost luată în consideraţie până când această supraveghere nu a devenit un *fait accompli*. Atunci când organizaţiile de apărare a libertăţilor cetăţeneşti s-au trezit, în sfârşit, începând să pună întrebări şi să dea glas neliniştilor lor, acestea au fost respinse violent de

adjunctul şefului poliţiei din City şi ministrul de interne. Când vine vorba de războiul antitero, nimănui nu-i mai pasă de sensibilităţile publicului. Vechile alei dimprejurul Băncii Angliei, „Bătrâna doamnă din Threadneedle Street", erau acum curăţate. Prostituatele din Cheapside şi Barbican au ales fie să renunţe la meserie, fie să se mute în Tower Hamlets, Southwark sau West End. În timp ce fraudele şi infracţiunile financiare au rămas la fel de obişnuite ca şi înainte, jafurile armate, furturile şi actele de violenţă stradală au devenit amintiri în City. Atunci când atrocităţile comise de IRA au continuat în provincie şi în West End, şi mai multe resurse au fost folosite pentru a proteja inima de aur a Capitalei, iar supraveghetorii au fost instruiţi să îmbunătăţească performanţele sistemelor lor cu ajutorul unui program care recunoştea şi atenţiona poliţia asupra prezenţei unei maşini furate în nici trei secunde de la intrarea ei în City.

Sistemul de supraveghere din City, cu programul său de identificare automată a numerelor de maşină, s-a dovedit o piedică de succes în calea atacurilor cu maşini-capcană şi urmează să fie extins în întreaga Mare Britanie, într-o primă fază în 23 de unităţi de poliţie din Anglia. Teoretic, sistemul va fi utilizat pentru a da de urma celor opt milioane şi jumătate de maşini care fie nu sunt cu taxele la zi, fie nu sunt asigurate, fie sunt suspectate de conexiuni cu activităţi infracţionale sau cu terorismul. Camerele de supraveghere, acum capabile de a monitoriza 3 500 de autovehicule pe oră, vor fi instalate în puncte fixe şi montate în dube ale poliţiei. Ele caută nu atât şoferi proşti, cât infractori motorizaţi. Totuşi, există o varietate de sisteme active, inclusiv unul constând dintr-o serie consecutivă de camere ascunse, care cronometrează un autovehicul de-a lungul unui kilometru şi jumătate de şosea. Sistemul este astfel conceput încât să se ocupe de maşinile cu viteză care încetinesc atunci când şoferii ştiu că se apropie o cameră de înregistrare, pentru că prin el se poate calcula viteza medie a autovehiculului pe parcursul

întregului traseu. Autorităţilor le place acest sistem, deoarece el nu face nici o discriminare. Programul nu se întreabă dacă vinovăţia şoferului în chestiune merită pusă la îndoială sau nu, el nu poate judeca subiectiv, precum un ofiţer de poliţie în uniformă. Nu există decât două opţiuni: încalci legea sau nu.

Sistemele de supraveghere şi tehnologiile se îmbunătăţesc permanent; deja nu mai există nimic care să oprească poliţia şi serviciile de securitate să conecteze sistemul la baza de date a Autorităţii pentru Şoferi şi Autovehicule (DVLA) din Swansea (Ţara Galilor), în care se regăsesc numele şi adresa fiecărui posesor de maşină din ţară. Aceasta le va permite poliţiştilor nu numai să tragă pe dreapta automobilişti, pentru tichete de parcare neplătite sau amenzi datorate depăşirii vitezei regulamentare, ci şi să urmărească traseele lor zilnice. Pericolul în ceea ce priveşte libertăţile cetăţeneşti este că astfel li se oferă posibilitatea agenţiilor de păstrare a ordinii publice – şi, ca atare, statului – de a-şi construi o imagine cuprinzătoare asupra deplasărilor şi comportamentului nostru, precum şi de a trage concluzii despre noi, pe baza datelor înregistrate. Această analiză nu este realizată de un comitet sau de un funcţionar aşezat la un birou, ci de un computer, care a fost programat să ajungă la nişte concluzii pornind de la date provenind din diferite surse. Un exemplu este sistemul Carnivore, utilizat de FBI, care înregistrează obiceiurile de lectură ale unei persoane, pe baza fişelor de bibliotecă şi a achiziţiilor de cărţi. Odată ce se ştie ceea ce citim, nu mai e decât un mic pas până la formarea unei opinii asupra încrederii şi adeziunii noastre politice. Iar aici libertatea se sfârşeşte.

Supravegherea de rutină a mulţimii, prin utilizarea unei televiziuni cu circuit închis (CCTV), devine chiar şi mai îngrijorătoare atunci când este combinată cu alte invenţii recente. Acum, Ministerul de Interne şi serviciile de securitate ascultă în mod curent convorbirile telefonice, fără a mai avea nevoie

de vreun mandat acordat de un judecător. De asemenea, se experimentează programe concepute pentru a identifica feţele oamenilor, pe baza unei arhive de poze, ale căror surse sunt rapoartele de arestare, Biroul Paşapoarte şi alte agenţii guvernamentale ce solicită identificarea fotografică. Tehnologia este deja utilizată de industria jocurilor de noroc din Statele Unite şi este în curs de introducere, în taină, într-unul sau două cazinouri din Londra. Această industrie practică frecvent schimbul de informaţii despre jucătorii suspectaţi că ar trişa. Jocul 21 sau ruleta sunt în mod special vulnerabile în special când sunt profesionişti în joc, aşa că participanţii sunt urmăriţi şi înregistraţi permanent. Jucătorii nedoriţi, aflaţi pretutindeni pe lista neagră, sunt filmaţi pe ascuns şi identificaţi imediat ce intră în clădire, iar apoi le este refuzat accesul în sala de jocuri. Panica generată în rândul personalului de securitate de căderea unui sistem de supraveghere este groaznic de urmărit. Totuşi, acurateţea recunoaşterii faciale este discutabilă, spre deosebire de testul ADN sau de înregistrarea irisului.

De la începuturile campaniei IRA din anii 1970, apoi după apariţia în Europa a unor varii grupări teroriste locale (ca Brigăzile Roşii în Italia sau Facţiunea Armata Roşie în Germania), măsurile de protecţie a intimităţii şi a datelor personale au fost lăsate deoparte, în mod frecvent, în momentele de alertă naţională. Fiecare regulă încălcată tinde să rămână aşa mult timp după ce ameninţarea aparentă a fost înlăturată sau s-a dovedit a fi inexistentă. De pildă, istoria detenţiei suspecţilor de terorism în închisoarea Long Kesh din Irlanda de Nord, în anii 1970, a făcut ca ministrului de interne să-i fie mai uşor, trei decenii mai târziu, să-i întemniţeze pe extremiştii islamici în închisoarea Belmarsh şi să-i ţină acolo fără să le fie intentat proces. Informaţiile strânse pentru propusa bază de date a cărţilor de identitate vor fi disponibile şi pentru alte agenţii guvernamentale, precum Administraţia Financiară sau Departamentul

Vamă şi Accize. Pe măsură ce perceputa ameninţare teroristă creşte, presiunea exercitată asupra literei legii de către politicieni devine tot mai puternică. Am asistat deja la intense presiuni de a desfiinţa sistemul cu juraţi şi prezumţia de nevinovăţie pentru multe infracţiuni, atât aici, cât şi în Statele Unite. Cât va mai dura oare până când un ministru britanic de interne se va împotrivi dorinţelor serviciilor de securitate şi va cere includerea convorbirilor telefonice înregistrate printre dovezile acceptabile în justiţie?

Principala justificare oferită pentru toate aceste atacuri asupra libertăţilor individuale este ameninţarea terorismului, care astăzi, după 9/11, poate scuza orice măsură extremă. Atunci când guvernul exagerează sau minte în ceea ce priveşte această ameninţare, pătrundem într-o epocă periculoasă a istoriei.

În tinereţea mea, când Churchill era prim-ministru, ideea că el ar minţi poporul pentru a intra în război era de neconceput. O fi fost el un bătrân ticălos, dar niciodată nu existase vreo îndoială că ţinea la interesele naţiunii. Churchill era un luptător şi un soldat. Fusese educat să-şi servească ţara şi stătuse în captivitate, ca prizonier de război, în Africa de Sud. Astăzi în schimb, deşi încă nu prea pare să ne pese, suntem conduşi de politicieni pentru care interesele de partid şi dorinţa personală de putere sunt mai presus de orice.

Introducerea noilor cărţi de identitate în Marea Britanie este mult mai importantă decât ni se pare. Prin această măsură, deplasările şi activităţile fiecărui cetăţean pot fi înregistrate şi arhivate în baze de date pentru securitate, care vor fi operate de companii private de securitate. Pe măsură ce tehnologia evoluează, va veni o vreme – mai devreme decât ne aşteptăm – în care un fişier electronic conţinând datele noastre de sănătate, limita de creditare bancară, călătoriile în străinătate, voturile la alegeri, alături de fiecare mişcare sau decizie pentru care trebuie să prezentăm un act de identitate, va fi disponibil

unui funcționar civil și, deci, unui politician, care s-ar putea să nu aibă la inimă interesele noastre. Este greu de înțeles ce avantaje va oferi cetățenilor un asemenea sistem. În cazul unei amenințări teroriste autentice, este ridicol să ne imaginăm că un sinucigaș cu bombă foarte hotărât va fi împiedicat de necesitatea de a deține o bucățică de plastic. Politicienii ne spun că aceste cărți de identitate ne vor ajuta să ne protejăm granițele de cei nepoftiți, dar se pare că nimeni nu s-a gândit la problema graniței libere dintre Republica Irlanda și Marea Britanie. Pe de altă parte, cunoașterea este putere, nu-i așa?, iar politicienii de azi vor găsi o cale de a ieși din această dilemă. Baza de date cu cărți de identitate, împreună cu toate bazele de date asociate ale agențiilor guvernamentale, va da statului o putere fără precedent de a-și băga nasul în viețile noastre private.

De la distrugerea World Trade Center, spaima de terorism a devenit o parte a dietei noastre politice zilnice, un adevărat *raison d'être* pentru nenumărate exemple de exces politic. Oamenii din umbră, experții în tehnologie și stăpânii lor politici au acum un cuvânt greu de spus în viețile noastre, atât aici, cât și în SUA. Supraveghetorilor le stă în fire să strângă și să arhiveze tot ce pot afla despre noi, iar apoi să țină secrete datele deținute. Despre asta vorbește această carte.

CAPITOLUL I

Tu cumperi, noi veghem

Cu mulţi ani în urmă, viaţa cotidiană era o chestiune mai degrabă simplă. Lumea mergea la muncă, se ducea în oraş să cumpere fructe şi legume de la piaţă, pâine de la brutărie şi carne de la măcelărie. Era cu totul de neconceput ideea că, într-o zi, ai putea fi filmat în timp ce te duci la muncă, fotografiat în timp ce conduci maşina, monitorizat în timp ce îţi alegi şi plăteşti cumpărăturile, că ar putea exista carduri de loialitate care să te individualizeze şi baze de date care să fie actualizate când îţi plăteşti facturile. Dar iată că toate acestea s-au întâmplat oricum. Practic, tot ceea ce facem este înregistrat şi stocat undeva. Iar nouă nu s-ar zice că ne pasă prea mult. Probabil, pentru că nu ne dăm seama în ce măsură renunţăm, zi după zi, la propria intimitate. La urma urmei, n-am greşit nimănui cu nimic, aşa că nu avem de ce să ne temem. Aşa să fie oare?

În cursul ultimilor 30 de ani, supravegherea informatizată a centrelor oraşelor, ca măsură de luptă împotriva terorismului, a crescut constant şi aproape fără nici o restricţie, cu efecte dramatice asupra vieţii urbane din Marea Britanie. Nimeni nu pare a şti cu exactitate câte camere de supraveghere ne urmăresc, însă chiar şi cele mai optimiste estimări sunt de ordinul milioanelor. Clive Norris, profesor de criminologie la Universitatea din Hull, a publicat recent propria analiză pe marginea acestui subiect. Numărul camerelor de filmat active în spaţiul

public din Marea Britanie a fost estimat de el la trei milioane. „Este dificil să furnizezi o cifră exactă. Nu toate sistemele de supraveghere se încadrează în Legea protecției datelor, dar credem că o aproximare moderată ar fi între două și trei milioane de unități de înregistrare individuale. Altfel spus, cam două camere la 30 de oameni“, susține Simon Davies, director al organizației de apărare a drepturilor omului Privacy International. Se spune că britanicul de rând este filmat în medie de până la 300 de ori pe zi, ceea ce face din Marea Britanie cea mai supravegheată societate de pe fața Pământului. De fapt, nu avem nici cea mai mică idee de câte ori intrăm în obiectiv fără voia noastră.

Știm că suntem filmați când călătorim cu trenul ori cu mașina, în supermarketuri, parcări și bănci, când mergem la un meci de fotbal sau când folosim un bancomat, când facem exerciții într-o sală de fitness sau când intrăm într-un tribunal, când trecem prin centrul orașului ș.a.m.d. Dar nici unul dintre noi nu poate ști cu certitudine de câte ori suntem filmați, în secret, de poliție sau de serviciile secrete ori ilegal, de persoane fizice, din rațiuni financiare. Însă faptul că nu se pot furniza date precise privind supravegherea din umbră nu schimbă cu nimic lucrurile. Supravegherea oficială reprezintă un motiv suficient de îngrijorare, un exemplu în acest sens fiind camerele instalate în dreptul stațiilor de autobuz. Dacă ești atent când treci prin dreptul magazinelor pe orice arteră urbană aglomerată, îți vei face o idee în legătură cu cine sunt aceia care îți înregistrează plimbarea și din ce motive.

Cele mai multe magazine de desfacere fac parte din asociații care practică schimbul de informații. Când situația o impune, ele colaborează pentru a urmări anumite persoane pe perioade îndelungate și pentru a obține date digitale complete despre unde s-au oprit acestea pe durata plimbării lor pe strada în cauză. Există numeroase moduri prin care se poate urmări traseul unei persoane.

Kensington High Street din vestul Londrei, de pildă, este una dintre cele mai supravegheate străzi din capitală. Este o zonă de lux de vreun kilometru şi jumătate, odinioară loc de promenadă al văduvelor înstărite şi al pechinezilor acestora, în prezent un paradis al cumpărătorilor; aici se mai află sediul *Daily Mail* şi al mai multor ambasade. Porneşte de la Royal Garden Hotel şi îndreaptă-te către Holland Park. Ridică-ţi privirea la zidurile din zona recepţiei hotelului şi, undeva deasupra celor mulţi care aşteaptă să îşi primească ori să îşi predea camerele de hotel, vei vedea o jumătate de duzină de cutii negre suspendate. Aceste cutii ascund lentilele mobile ale unor camere de luat vederi comandate de la distanţă.

Royal Garden este unul dintre hotelurile de top ale Londrei. Şefi de stat, oameni de afaceri străini, spioni, mercenari, celebrităţi înstărite şi excentrice formează clientela obişnuită a hotelului. Odată ce se cazează, ei vor să aibă posibilitatea de a se relaxa în camerele lor şi de a-şi vedea liniştiţi de treburi. În plus, doresc să se ştie în deplină siguranţă. Directorii celor mai mari hoteluri din lume se află în posesia mai multor secrete decât majoritatea oamenilor. Ei trebuie să satisfacă toanele preşedinţilor şi dictatorilor, ale vedetelor de film, ale starurilor rock şi ale scriitorilor împătimiţi de băutură, precum şi să păstreze confidenţial tot ceea ce văd. De asemenea, ei trebuie să facă în aşa fel încât oaspeţii lor să simtă că nu au de ce să se mai teamă din momentul în care au trecut de portarul în uniformă de la intrare. De aceea, directorii trebuie să se asigure că toţi cei care pătrund în hotel sunt filmaţi şi că îi pot supraveghea atât pe oaspeţi, cât şi pe vizitatorii lor, până în momentul în care părăsesc incinta.

La est de acest hotel se găsesc PalaceAvenue şi Kensington Palace Green. Cochetul drum care duce la palatul Kensington este străjuit de o parte de grădinile Kensington şi de cealaltă parte de grădinile Kensington Palace. Când ieşi din hotel şi

privești către peretele estic, vei vedea răsărind, ca niște ochi și urechi, camere și senzori ce au rolul de a acoperi zona de acces către apartamentele regale. Partea superioară a zidului este prevăzută cu sârmă ghimpată, pentru a preveni tentativele de deteriorare a echipamentului electronic ori de cucerire a unei poziții strategice în timpul vreunei parade. Colțul acesta al Hyde Park a fost locul în care mulțimea îndurerată a ridicat munți de flori în zilele ce au urmat morții prințesei Diana. Iată un punct vulnerabil al Marii Britanii. Alte camere de filmat ne așteaptă peste drum, în Bar Cuba, unde oaspeții hotelului dau fuga pentru a se bucura de plăcerile unui pahar de băutură mai ieftin.

Puțin mai la vest, grădinile Kensington Palace sunt păzite de gardieni în uniformă. Bulevardul străjuit de copaci este deschis publicului, dar nu poate fi parcurs de mașini, cu excepția celor cu număr de corp diplomatic, și este interzis tuturor muncitorilor care nu dețin o autorizație specială. Majoritatea misiunilor diplomatice importante se află aici, inclusiv Ambasada Rusiei, în capătul nordic. În fața unor clădiri s-au montat baricade antitanc, pentru a preveni atacurile cu mașini-capcană, iar farfuriile antenelor-satelit se înalță deasupra acoperișurilor, făcându-și loc printre ramurile platanilor. Bulevardul mărginit de copaci geme de camere de supraveghere și antene radio, în timp ce polițiști înarmați patrulează non-stop – un motiv temeinic pentru ca toți cei care se gândesc să recurgă la un protest în fața Ambasadei Japoniei să-și schimbe planurile.

Dacă decizi să te tratezi cu o cafea pe cealaltă parte a străzii Kensington High, la Barkers, cu marinura sa edwardiană, vei vedea fără îndoială tineri scriind la laptopuri ori vorbind la telefoanele lor mobile. La etaj, în impunătoarea clădire Northcliffe House, se află sediile publicațiilor *Daily Mail, Mail on Sunday* și *London Evening Standard.* Cu degajarea pe care ți-o dă practica îndelungată, jurnaliștii sunt în stare ca, de la birourile lor,

să asculte şi să vadă tot ce se întâmplă în cafeneaua de la parter şi chiar în hotel. Supravegherea şi securitatea sunt maxime şi făţişe în birourile *Associated Newspapers,* personalul fiind filmat în mod curent prin televiziunea cu circuit închis. Genţile şi servietele sunt percheziţionate, iar toate birourile şi coridoarele sunt împânzite cu camere de supraveghere. Testarea sistemului reprezintă o practică notorie printre jurnalişti. Atunci când s-a promulgat legea care interzice armele de dimensiuni mici şi cluburile de tir, unul dintre cei dintâi reporteri ajunşi în clădire, în chiar ziua intrării în vigoare a noii legi, a adus în redacţia de ştiri un uriaş revolver Webley Service (nefuncţional), susţinând că l-a găsit în lift. Măsurile de securitate valabile pentru întreaga clădire s-au înăsprit la scurt timp. Compania dispune de un personal de securitate redutabil, nu doar din pricina implicaţiilor politice ale activităţilor pe care le desfăşoară, ci mai ales din pricina secretelor pe care le deţine, dar alege să nu le divulge. Informaţiile reprezintă totul pentru un ziar de scandal cu difuzare naţională şi e un lucru bine ştiut că editorii şi directorii companiei îi pot oricând distruge sau pune într-o lumină cel puţin nefavorabilă pe unii dintre cei mai puternici oameni din Marea Britanie.

Informaţiile sunt, de asemenea, importante în josul străzii, la sucursala din Kensington a Marks and Spencer, unul dintre magazinele-cheie din Londra ale companiei. În faţa sa, zeci de femei şi copii se învârt încoace şi încolo, formând un grup imprevizibil şi zgomotos. Provin din Europa de Est şi vorbesc în limba lor. Copiii par a nu mai putea fi controlaţi, în timp ce femeile poartă *burka* lungi şi văluri care le acoperă feţele. Ne vom întoarce la ei în curând.

Spre deosebire de alţi comercianţi, Marks and Spencer nu obişnuieşte să ataşeze etichete de securitate mărfurilor sale, bazându-se, în schimb, pe supravegherea video şi pe agenţi de pază în uniformă ori detectivi de magazin în civil. Este un

sistem eficient. Rețeaua marilor magazine londoneze menține legături strânse între toate spațiile comerciale și raportează orice mișcare a unui grup de clienți considerați suspecți. Eficiența forței de securitate M&S și abilitatea sa de a acționa în cazul unui furt au fost testate și dovedite în timp. Când un grup de potențiali hoți de magazine ori de buzunare pleacă din Kensington, magazinele din Oxford Street îi așteaptă deja. Unitățile comerciale trebuie să se bazeze pe experiența și rețeaua de comunicare pe care le dețin, deoarece comunicarea din interiorul Poliției este considerată prea lentă.

Pentru mulți cumpărători pretențioși, magazinele din Kensington și Chelsea au un aer de respectabilitate neagresivă și un calm care le fac preferabile celor din Oxford, aflat la vreun kilometru și jumătate la nord-est, cu nebunia permanentă a reducerilor de acolo. Cu mult mai puțin evident este însă succesul lor în contracararea furtului organizat. Această luptă este neîntreruptă, prin urmare, neîntreruptă este și supravegherea clienților prin mijloace electronice. Fiecare persoană este înregistrată intrând, ieșind și plimbându-se prin magazin. Suma, dar și planificarea investită în sistemul de securitate al Marks and Spencer este, fără îndoială, imensă, și ne-ar surprinde pe toți. Din punct de vedere strict comercial, camerele de supraveghere par toate la fel, dar munca de supraveghere înseamnă mult mai mult. Dacă intri în încăperile de monitorizare ale M&S, nu vei găsi un munte de ecrane și agenți de securitate plictisiți, așteptând să li se termine tura. Fiecare magazin are zeci de camere de supraveghere, ale căror imagini sunt urmărite de persoane cu o pregătire minuțioasă, pe cel mai performant ecran unic de mari dimensiuni de pe piață. Tehnologia este cunoscută sub numele de „neurală“, ceea ce înseamnă că aceste camere digitale sunt capabile să discearnă activitatea suspectă de cea obișnuită, transmițând-o apoi pe prima operatorului. Programul izolează porțiunea relevantă de înregistrare și îi acordă prioritate, astfel încât

supraveghetorul să vadă imediat ce se întâmplă, să identifice persoanele suspecte şi să cheme în ajutor personalul de securitate din magazin. Este rapid, eficient şi incredibil de scump, dar acesta este viitorul supravegherii.

Dat fiind că poate izola anumite ameninţări de tiparele altminteri acceptabile de comportament, supravegherea neurală revoluţionează arta supravegherii electronice. Avantajele sunt multiple, nu în ultimul rând pentru că te scapă de grămezi de ecrane greu de administrat şi de o cantitate enormă de informaţii confuze. S-a stabilit că durata medie a vizionării active, de către poliţiştii londonezi experţi în CCTV de la sediul din Wood Lane, a imaginilor camerelor de supraveghere nu a fost mai mare de 20 de minute. Nimic nu le scapă camerelor neurale şi sistemului de „prevenire proactivă" pe care acestea se bazează, ce face ca informaţia primită să fie selectată şi afişată pe monitoare. Tot ce apare pe monitorul neural este relevant. Unicul operator de care sistemul are nevoie pentru a funcţiona lucrează izolat, într-un centru de comandă departe de locul supravegheat. El sau ea stă într-o cameră cu dotări spartane şi un singur ecran de perete, imens, pe care pot fi transmise imaginile, fiecare imagine cu codul ei de prioritate. Lumina este difuză, iar operatorul este aşezat într-un confortabil scaun cu spătar înalt, în faţa unei mese cu o grămadă de telefoane.

Acest sistem versatil are multe alte aplicaţii, pe lângă cele din sectorul comerţului. De pildă, închipuiţi-vă o uriaşă reşedinţă englezească în stil georgian, întinsă pe mii şi mii de hectare de păşune şi păduri, cu grădinile înconjurate de un zid înalt de cărămidă şi sârmă ghimpată, cu lăţimea de trei metri la bază. Cele patru intrări principale în parc sunt controlate electronic. Terenul şi pereţii casei sunt împânziţi cu camere de luat vederi şi cu senzori de mişcare. Interiorul casei este dotat, de asemenea, cu mici camere ascunse, fiecare dintre acestea fiind setată pentru a opera cu un sistem programat în prealabil. Întregul

material brut înregistrat de camere şi de senzori este transmis unităţii de monitorizare la distanţă, unde e filtrat şi evaluat de către sistem. Fiecare cameră înregistrează şi analizează activităţile care au loc într-un spaţiu precis definit. Camerele pot detecta mişcarea, urmări şi analiza comportamentul, pe baza sistemului integrat „extremitatea dinamică principală". Acesta presupune ca, atunci când se sesizează o anomalie, oricare ar fi natura acesteia, detaliile să fie afişate în camera de control, unde operatorul sistemului, aşezat în faţa unui ecran de perete imens, cu o imagine foarte clară, poate activa calea cea mai indicată de acţiune.

Fiecare cameră este programată pentru a considera acceptabile o serie de activităţi care au loc în raza sa de acţiune. Orice a fost indicat ca reprezentând un comportament suspect este izolat şi înregistrat, spre deosebire de restul tiparelor de acţiune. De exemplu, un bărbat care intră în parcarea din spatele proprietăţii. El poartă o geantă pe care o lasă pe jos, lângă un alt autoturism parcat. Apoi se întoarce şi pleacă, lăsând în urmă geanta. Sistemul interpretează imediat situaţia descrisă ca pe o ameninţare şi o retransmite instantaneu către operator, care va trebui să o analizeze. Geanta este scoasă în evidenţă şi prezentată haşurat pe ecran, astfel ca privirea care monitorizează să fie atrasă imediat de ea, iar operatorul să poată înţelege fără întârziere natura problemei. Sistemul îi furnizează o înregistrare video completă a momentelor care au precedat şi a celor care au urmat incidentului, permiţându-i să examineze în cele mai mici detalii atât geanta, cât şi persoana care pare a fi abandonat-o.

Acest sistem se numeşte Spectiva. Înregistrările sunt atât audio, cât şi video de calitate, existând posibilitatea izolării şi redării unei conversaţii anume dintr-o zonă extinsă. Privitorul primeşte orice detaliu de care are nevoie pentru a lua decizia necesară analizării a ceea ce s-a înregistrat şi să acţioneze în consecinţă. Dacă persoana care a penetrat perimetrul

înregistrării ar fi lăsat geanta jos doar pentru câteva momente, pentru ca apoi să o ridice şi să îşi vadă de drum, sistemul ar fi putut fi programat să ignore incidentul. Sistemul de supraveghere a fost programat pentru a acţiona în cazul unei game largi de posibilităţi sugerate de către firma de securitate care l-a instalat. De pildă, dacă, în timpul nopţii, o siluetă aleargă prin parcare sau intră în raza de acţiune a camerei de supraveghere şi se ghemuieşte în spatele unei maşini, incidentul va fi selectat şi afişat instantaneu operatorului. Dacă un copil aleargă în acelaşi loc ziua, ceea ce nu constituie în principiu nimic anormal, sistemul poate fi programat pentru a-l ignora. Dacă o persoană pare a purta o armă, camerele de supraveghere o vor recunoaşte ca atare şi vor reacţiona în consecinţă. De îndată ce comportamentul în cauză a fost analizat, sistemul va continua urmărirea subiectului. Îmbrăcămintea neadecvată, o mască de schi sau o vestă antiglonţ pot fi recunoscute, declanşând un răspuns corespunzător. Tehnologia recunoaşterii faciale a făcut posibilă amplasarea camerelor în aşa fel încât să permită stocarea conturului sau a caracteristicilor fizice ale tuturor vizitatorilor, cunoscuţi şi neinvitaţi, ai casei sau ai dependinţelor. Totuşi, tehnologia se află încă într-un stadiu incipient de dezvoltare şi poate fi contracarată prin folosirea unor articole de îmbrăcăminte sau a unor ochelari ce ascund chipul.

În cazul unei case particulare din mijlocul unui mare domeniu din Anglia rurală, prioritară este mai degrabă siguranţa familiei şi a proprietăţii, iar sistemul se poate să fi fost instalat la insistenţele asiguratorilor familiei. Prima dată când m-am confruntat cu eficienţa sistemului neural a fost la o casă particulară din Hampshire. Sistemul fusese instalat de către una dintre cele mai mari firme de supraveghere, CSS, cu sediul în Southampton. O mare plăcere a proprietarului casei a fost să-mi arate cum îşi poate monitoriza proprietatea oriunde s-ar afla în lume, prin intermediul laptopului sau al unui palmtop.

Bunăoară, aflat într-un hotel în Tokio, utilizând tehnologia wireless şi propriul laptop, el poate comunica şi controla camerele de supraveghere. Dacă vrea, poate urmări orice anomalie semnalată de sistemul neural. Instalaţia sa Cieffe, de provenienţă italiană, oferă posibilitatea vizionării integrale a înregistrărilor pe un monitor virtual şi a activării comenzilor de la mare distanţă. Privind sistemul la lucru într-un bar din City, în compania proprietarului, am putut citi minuscula inscripţie de pe autocolantul de plată a asigurării vehiculului, filmată de o cameră situată la 100 de metri de maşină, pe peretele posterior al casei. Pe de altă parte, facilitatea de a capta sistemul şi de a recepţiona imagini cu propria casă şi cu membrii familiei este menită a servi exclusiv confortului psihic al proprietarului, deoarece sistemul este monitorizat 24 de ore pe zi de personalul CSS, cu care acesta poate intra în contact prin simpla apăsare a unui buton.

Înainte de a-l consilia pe proprietar, CSS a analizat vulnerabilitatea casei de la ţară. Reprezentanţii firmei au dotat sistemele complete, dar discrete, de detectare a încălcării perimetrului, cu CCTV proactiv, care transmite semnale unui dispecerat central. Compania foloseşte serviciile unor operatori cu experienţă, care pot răspunde pe loc oricăror ameninţări la adresa casei sau a bunurilor din interiorul acesteia. Robert Fiorentino, responsabilul CSS în Southampton, proiectează sisteme de securitate la comandă. „Putem face ceea ce Poliţia este adesea incapabilă să facă, adică să protejăm locaţii vulnerabile şi să prevenim infracţiuni grave“, a declarat el. De exemplu, în cazul unui atac de proporţii asupra unei proprietăţi, informaţiile sunt selectate de către sistem şi afişate pe ecran într-o selecţie de imagini prioritare, dându-i astfel operatorului suficiente amănunte pentru a-şi putea face o imagine completă asupra incidentului. În calitate de agenţie privată, CSS nu este condiţionată de sistemele puternic birocratizate de raportare a datelor, dar

respectă Legea protecţiei informaţiilor, precum şi orice alte legi şi regulamente care normează furnizarea dovezilor în cadrul unui proces. Tehnologia neurală utilizată în supraveghere este privită în industrie ca fiind mai degrabă preventivă decât reactivă – un important pas înainte în securizarea proprietăţii.

Scopul dintâi al sistemelor precum cel proiectat de CSS este de a preveni infracţiunile săvârşite în spaţii publice. În SUA, eforturile de a stabili o legătură între căutarea neurală, detectarea şi supravegherea mişcărilor, pe de o parte, şi tehnici precum recunoaşterea facială şi tehnologiile sateliţilor de poziţionare globală (GPS), pe de altă parte, sunt în desfăşurare de mai bine de doi ani, în cadrul unei iniţiative a Departamentului de Securitate Internă. Obiectivul este dezvoltarea unui sistem care se poate aplica pe o stradă aglomerată, pentru prevenirea unui posibil atac terorist.

Tehnologiei supravegherii neurale i se aduc permanent îmbunătăţiri, preţul acesteia scade constant, iar personalul însărcinat cu operarea sistemului are parte de o pregătire din ce în ce mai sofisticată. Nu peste mult timp, acest sistem va ajunge să fie folosit de toate marile magazine, iar informaţiile pe care le furnizează vor fi coroborate cu cele ale bazelor de date ale infractorilor cunoscuţi. Nu ar trebui să ne mire interesul comercianţilor pentru dezvoltările aplicaţiilor de securitate care oferă facilitatea de a selecta imaginile, reducând astfel personalul angajat. În perioadele aglomerate, la sfârşit de săptămână, marile magazine din West End devin câmpurile unui război comercial de gherilă, informaţiile privind infractori cunoscuţi sau suspecţi fiind transmise, de la un distribuitor la altul, în întreaga zonă. La orele de vârf, echipajele de poliţie patrulează de-a lungul străzii şi în staţia de metrou. În lunile de vară, magazinele din Kensington sunt vizitate regulat de grupuri de hoţi, printre care mulţi veniţi din Europa de Est şi Balcani. Aceştia acţionează în grupuri mici. Linia de atac este formată

adesea din femei și copii, ajutați de bărbați care conduc mașini rapide, în susul și în josul străzii. Fetele și băieții prepuberi implicați sunt antrenați intens, pentru a deveni ași ai furtului de buzunare (altfel spus, ai „ciordelii“), pentru a învăța cum să părăsească locul faptei și să distragă atenția victimelor. Au asupra lor identități false, pentru a-i convinge pe polițiști și pe detectivii de magazin că sunt minori, pretinzând de asemenea că nu cunosc limba engleză. Operează în echipe și sunt foarte îndemânatici. Traseele lor de retragere sunt stabilite minuțios și repetate conștiincios.

În încercarea de a contracara amenințarea hoților din magazine, de îndată ce apare cel mai mic indiciu al unui incident sau un infractor cu cazier este recunoscut, sunt alertați pe loc toți comercianții de pe stradă, precum și unitățile poliției de combatere a furturilor din magazine din Kensington și Notting Hill. Mai multe lanțuri mari testează în prezent supravegherea pe baza recunoașterii faciale, ca mod de a identifica și de a lua măsuri împotriva hoților profesioniști. Deși este mană cerească pentru sistemele de securitate, identificarea facială mai are încă mult până să-și dovedească infailibilitatea.

În prezent, Londra este cel mai supravegheat oraș din lume. Pe lângă cele două milioane de camere cu circuit închis, există opt elicoptere de supraveghere ale poliției – și alte două în pregătire –, prin intermediul cărora se pot transporta rapid, practic oriunde în capitală, echipaje înarmate. În funcție de gradul de vulnerabilitate, s-au format zone de securitate, unele supravegheate mai intens decât altele. Polițistul cu baston și fluier care patrulează pe stradă a devenit un exponat de muzeu. Urmașul său modern este dotat cu motocicletă rapidă, sisteme de comunicare de ultimă oră și echipament atât defensiv, cât și ofensiv.

Sistemul chiar funcționează. Recent, am însoțit doi polițiști pe bicicletă ai Poliției londoneze în Aldersgate, unde ei au observat

un domn mai în vârstă, mergând hotărât în direcţie sudică. „Îl cunosc“, a spus unul din tovarăşii mei, un sergent musculos, îmbrăcat în galben reflectorizant, cu vestă antiglonţ şi spray paralizant, baston, pistol cu electroşocuri şi trusă de prim ajutor. „Blochează telefoanele publice cu bucăţi de plastic şi se întoarce mai târziu pentru a strânge banii; l-am mai săltat acum vreo câţiva ani.“ El a luat legătura cu unitatea de monitorizare prin televiziune cu circuit închis, cu ajutorul radioului încorporat în cască. „E un bătrân în impermeabil galben, care se plimbă prin Aldersgate, la vreo 45 de metri sud de Long Lane, îl vedeţi pe ecran?“ După nici 20 de secunde, bărbatul era urmărit prin intermediul camerelor, în prim-plan şi cu maximum de detalii, din camera de supraveghere de pe Wood Street. L-am urmărit de la distanţă, în timp ce camerele de supraveghere îl înregistrau cum a luat-o pe Grubb Street şi apoi pe Cheapside, unde s-a oprit pentru a se uita la o vitrină. Poliţiştii s-au dus să îl întrebe de sănătate, în timp ce eu priveam. Un al treilea poliţist pe bicicletă, o femeie sergent, s-a înfiinţat şi ea lângă ei, pe trotuar, deşi n-aş putea spune de unde apăruse. După alte câteva minute, un alt poliţist a apărut la faţa locului. Din senin, strada se umpluse de poliţişti pe bicicletă.

Nu am asistat la comiterea vreunei agresiuni, poliţiştii au fost toţi amabili şi politicoşi, însă asta după ce îl urmărisem pe acel bărbat preţ de 30 de minute şi după ce acesta fusese filmat în ascuns şi cu mare acurateţe, din Aldersgate până în Cheapside. Susţinea că munceşte în Finsbury Square şi că are tabietul de a ieşi la plimbare în fiecare zi, la ora prânzului. Însă omul nu se afla la prima confruntare cu poliţia şi, după cum a spus apoi unul dintre oamenii legii, „dacă în viitor va mai dori să facă ceva necurat, o să se gândească de două ori înainte. Îi ştim numele şi adresa“. Asta mai însemna că acest incident minor fusese înregistrat şi că trăsăturile faciale ale bărbatului fuseseră stocate în baza de date a poliţiei, de unde, printr-o singură apăsare a unei taste, puteau fi reactualizate şi adăugate în baza lor de date de recunoaştere

facială. Protagonistul acestui episod neînsemnat, dar antrenant, nu avea nici cea mai vagă idee că plimbarea lui de prânz tocmai fusese înregistrată pentru posteritate sau că propria figură putea fi afişată pe un ecran de computer nu numai din Londra, dar în curând şi din orice stat cu care s-au semnat acorduri în domeniu, chiar şi după ce el va fi fost de mult oale şi ulcele.

Sistemul de supraveghere din City, cu program de recunoaştere automată a numărului de înmatriculare, va fi în curând implementat în 23 de secţii din Anglia, iar apoi în toată Marea Britanie. Teoretic, sistemul va fi utilizat la scară naţională pentru a monitoriza cele opt milioane şi jumătate de maşini pentru care nu s-au plătit taxe, neasigurate ori suspectate de a fi utilizate pentru infracţiuni sau terorism. Camerele pot monitoriza în prezent 3 500 vehicule pe oră şi vor fi instalate atât în locuri fixe, cât şi montate pe dubele poliţiei. Însă nu există absolut nici o garanţie a faptului că utilizarea sistemului se va limita la găsirea „adevăraţilor" infractori.

Tehnologia de supraveghere este îmbunătăţită permanent. Deja nimic nu poate opri poliţia şi serviciile secrete de la a conecta sistemul la baza de date a Autorităţii pentru Şoferi şi Autovehicule (DVLA), în care se regăsesc numele şi adresa fiecărui posesor de maşină din ţară. Aceasta nu numai că ar accelera ritmul arestărilor pentru neplata parcării sau a amenzilor pentru depăşirea limitei de viteză, dar ar facilita şi urmărirea traseului zilnic al şoferilor. Pericolul la adresa libertăţilor cetăţeneşti rezidă în aceea că încurajează poliţia şi, implicit, statul să înregistreze tiparele noastre de comportament şi, pe baza înregistrărilor, să tragă concluzii.

În timp ce City-ul reprezintă probabil unul dintre peisajele urbane cel mai intens supravegheate şi păzite din lume, Kensington Street nu diferă prea mult de orice altă arteră importantă a Marii Britanii. Mergi pe Kensington şi sigur vei fi permanent supravegheat de vreo cameră. Intră într-un magazin sau într-un

restaurant şi vei fi preluat de un alt sistem de supraveghere. Pretutindeni în jurul tău se desfăşoară această luptă între comercianţi şi infractori, iar tu te afli, fără voia ta, în mijlocul ei, doar pentru că te-ai nimerit pe acolo şi vrei să cheltuieşti nişte bani. Prin lege, imaginea ta ar trebui ştearsă din sistem în termen de 31 de zile, însă nimeni nu este desemnat să verifice dacă acest lucru se şi întâmplă. Când îţi foloseşti cartea de credit pentru a-ţi plăti cumpărăturile şi îţi arăţi cardul de fidelitate la casă, tranzacţia durează suficient pentru ca imaginea ta înregistrată să poată fi corelată cu detaliile cardurilor tale. Proprietarii magazinului pot afla cu uşurinţă unde trăieşti, ce servicii bancare utilizezi, câţi copii ai şi încă multe altele, prin simpla confruntare a înregistrărilor de pe camerele de supraveghere cu cele din rapoartele casierilor.

Astăzi nici pe stradă nu trebuie să vorbeşti ce nu trebuie, pentru că tot ce spui poate fi interceptat prin telefonul tău mobil, analizat şi catalogat drept opinie personală, astfel încât te poţi trezi trecut pe lista de persoane considerate indezirabile de către stat. Şi nu trebuie să te temi doar de serviciile secrete, ci şi de mass-media din Marea Britanie. „Conversaţiile private“ de altădată, acelea pe care nimeni altcineva nu le mai putea auzi, au devenit un vis frumos. Nu mai există legătură telefonică sigură, internetul se oferă larg interceptării, iar e-mailurile au devenit bun comun. Dacă nu cumva stai lângă o cascadă, protejat de un cordon de agenţi de securitate surzi, care au fost percheziţionaţi pentru a nu purta cu ei dispozitive de înregistrare şi care formează în jurul tău un cerc cu diametrul de cel puţin 200 de metri, atunci nu ai nici o garanţie că discuţia confidenţială cu prietenul tău sau cu nevasta acestuia va rămâne între voi. Şeful MI5 comunică cu prim-ministrul prin intermediul unor informări scrise de mână şi livrate personal de către un curier la Camera Comunelor. Chiar dacă îţi iei toate măsurile de precauţie posibile, tot nu poţi băga mâna în foc pentru confidenţialitatea unei comunicări.

Se prea poate ca un dispozitiv de înregistrare audio sau de monitorizare a mișcării să fi fost instalat în podea sau în vreun tufiș din apropiere. E la fel de posibil ca un satelit să te filmeze sau ca un aparat aeropurtat în miniatură fie să te asculte, fie să îți înregistreze mișcările gurii, pentru ca apoi să le traducă în cuvinte.

Telefoanele mobile sunt interzise în cluburi private, în săli de judecată, în unele întruniri de afaceri și politice nu doar pentru că sunt iritante, ci pentru că pot fi prevăzute cu camere care pot filma sau fotografia ori cu funcții de înregistrare audio. Cele mai multe telefoane mobile moderne sunt suficient de avansate pentru a înregistra conversații din vecinătate. Dispozitive miniaturale, digitale, cu activare la voce, cum este Olympus DS330, pot fi cumpărate în Londra, pe Tottenham Court Road, cu 100 de lire sterline. Ascunse în buzunar, ele pot înregistra conversații într-un local zgomotos, eliminând sunetele nedorite de fundal. Dacă rețelele de supraveghere și interceptare a convorbirilor sunt supuse Legii protecției datelor și legislației privind drepturile omului, nimeni nu poate ști câte persoane private ori companii utilizează astfel de dispozitive pentru a înregistra activitățile pe care le derulezi. Câte hoteluri efectuează regulat controale de siguranță pentru a depista eventualele camere de supraveghere ori microfoane? Aproape nici unul. Dacă soliciți servicii de această natură marilor hoteluri londoneze, ei vor angaja o echipă de specialiști. Dar asta numai dacă o ceri în mod expres și, oricum, la un preț prohibitiv. Desigur, ei ar prefera să îți rezolvi singur problema, dat fiind că nu pot garanta siguranța antiinterceptare a camerelor și, dacă într-adevăr *ești* înregistrat, atunci hotelului i s-ar putea imputa daune. Și cât de des ar trebui să fie controlată camera ta? Zilnic? De două ori pe zi? Poate cineva garanta că firma de securitate angajată să-ți verifice dormitorul este destul de eficientă pentru a depista lentilele din fibră optică aflate probabil în spatele oglinzii de la baie? Dar dacă lucrează pentru altcineva? Chiar și o verificare internă s-ar

putea dovedi insuficientă. Dispozitivele de ascultare cu rază lungă de tip Sentinel pot fi îndreptate către fereastra unui dormitor, transformând vibraţiile percepute în unde sonore. Şi, în fond, cum îl poţi împiedica pe un jurnalist echipat cu cele mai scumpe dotări disponibile în comerţ să-ţi asculte conversaţia, dacă el chiar ţine morţiş să o facă? Patronii săi deţin resursele pentru a achiziţiona echipamente mai sofisticate decât cele la care ar putea visa vreodată serviciile de informaţii.

Elizabeth Hurley, ca orice vedetă, a avut multe probleme de acest gen. „Personal, nu cunosc nici o celebritate căreia să nu îi fi fost ascultate convorbirile“, a declarat ea recent. „Toţi caută permanent şi pretutindeni microfoane. Asemenea traficanţilor de droguri, toţi avem telefoane pe bază de amprentă digitală, fără număr înregistrat, însă mi s-au interceptat inclusiv convorbirile la telefonul fix, aşa că acum nu mai vorbesc la telefon. Dacă vreau să mă întâlnesc cu cineva şi să am o conversaţie privată, atunci întâlnirea va avea loc pe un pod. S-a ajuns până la a mi se planta microfoane în camera de hotel. Sunt bani buni la mijloc pentru aceşti rataţi care nu ştiu cum altfel să câştige o pâine.“

Interceptarea convorbirilor celebrităţilor nu este o invenţie de dată recentă. Koo Stark mi-a mărturisit, la un moment dat, că i s-a ascultat telefonul în perioada în care era partenera ducelui de York. „Ştiam că cineva ne asculta convorbirile, deoarece *Daily Mail* a publicat detalii ale unei conversaţii care nu puteau fi obţinute altcumva. Era o problemă gravă, fiindcă ştiam că dispozitivul nu fusese montat în casă, aşa că serviciul de pază a trimis experţi în supraveghere, iar ei au dezgropat un microfon pe linia telefonică terestră din dreptul casei, cam la 20 de metri de locuinţa mea, într-un grajd aflat la nord de Belgrave Square. Ştiam cu siguranţă că aceasta reprezintă una din măsurile de supraveghere puse la cale de David English de la *Daily Mail*. Ar fi făcut orice să afle până şi cel mai nesemnificativ amănunt despre noi. Este oarecum bizar, dar, când îţi dai seama că ai

fost urmărit, devii foarte precaut în privința locurilor unde vorbești cu oamenii. Nicăieri nu mai ești în siguranță."

Celebritățile ar deveni încă și mai paranoice – și pe bună dreptate – dacă ar ști că deseori polițiștii sunt aceia care furnizează informații reprezentanților mass-media. La începutul lui 2005, o rețea de foști polițiști londonezi, incluzând un operator al sistemului de supraveghere și mai mulți detectivi particulari, a fost condamnată pentru vânzarea numerelor de înmatriculare ale unor vehicule, precum și a unor date obținute de la Biroul de Informații privind Infractorii (CRO – Criminal Records Office). Datele transmise includ detalii privind mai multe vedete de televiziune, precum și detalii cu privire la infracțiunile rutiere comise de conducătorul unui autocar implicat într-un accident pe teritoriul Franței. Deși aceste date nu par a avea cine știe ce greutate, ele au servit la susținerea unor articole speculative apărute în ziare de scandal. Aceasta reprezintă o demonstrație a faptului că e extrem de ușor să încalci regulile, și că o informație altfel minoră poate fi utilizată pentru a da o spoială de veridicitate unui articol prost documentat, astfel încât acesta din urmă să poată fi publicat. De pildă, detalii privind proprietarul unui scuter folosit de un lider sindical pentru a circula în Londra în timpul grevei angajaților de la metrou au fost transmise lui Paul Marshall, responsabil cu relațiile publice la o secție de poliție din sudul Londrei, care le-a oferit lui Alan King, fost polițist, iar acesta, la rândul său, le-a vândut unui jurnalist. În timpul procesului, judecătorul a apreciat că siguranța informațiilor clasificate depinde de buna-credință a numărului mare de polițiști care le manipulează. Procesul, care s-a ținut la Tribunalul Regal Blackfriars, unde cei patru acuzați au fost condamnați, a demonstrat că există o piață largă de desfacere pentru materialele secrete aflate în posesia poliției. Cererea va crește odată ce baza de date computerizată a poliției va deveni mai mare și mai accesibilă hackerilor și cyberteroriștilor.

Aşadar, în timp ce ţi-ai făcut cumpărăturile pe Kensington, ai fost filmat, iar tranzacţiile pe care le-ai derulat au fost înregistrate. A sosit timpul să te întorci acasă. La staţia de metrou Kensington High Street, uşă în uşă cu Marks and Spencer, 25 de camere înregistrează tot ce intră şi iese. Când pasagerii se înghesuie să treacă de turnichet, folosind cardul de transport în comun, ei lasă în urma lor o amprentă care nu poate fi ştearsă. Poliţiştii de la Transporturi şi cei de la secţia din Kensington de pe Earls Court Road se amestecă printre navetişti. În timp ce îi caută pe hoţii de buzunare care se pierd în vasta reţea subterană, ofiţerii de la faţa locului primesc permanent date de la cei care monitorizează camerele de supraveghere, prin intermediul frecvenţei radio alocate poliţiei.

Un tur pe orice stradă aglomerată suscită automat o senzaţie de nervozitate acută, de îndată ce îţi dai seama de numărul semnalelor şi urmelor care plutesc în aer, deasupra ta. De fiecare dată când foloseşti o carte de credit, un „card inteligent“ sau un telefon mobil, de fiecare dată când dezactivezi sistemul de închidere a maşinii cu telecomanda, poziţia ta exactă pe hartă poate fi stabilită şi înregistrată, iar mişcările şi acţiunile tale pot fi urmărite cu maximum de acurateţe. Mergi pe o stradă din vestul Londrei şi vei putea observa senzorii care absorb şi transmit informaţiile către baze de date publice şi private. Odată înregistrate informaţiile, ele pot fi transmise instantaneu poliţiei, serviciilor secrete şi firmelor de pază. Amprentele electronice pe care le lăsăm în urma noastră ne-au schimbat pe veci viaţa. Totuşi, cei mai mulţi dintre noi nu suntem conştienţi că nu am mai trăit niciodată într-un astfel de mediu.

În industria computerelor, există o maximă cunoscută sub numele de Legea lui Moore, care spune că performanţele computerelor se dublează la fiecare 12 luni. Aşa că vor exista destule pârghii de silicon pentru a procesa şi a analiza chiar toate datele personale. Iar acum că *Ei* deţin informaţiile, ce vor face cu ele? Şi totuşi, cine sunt *Ei?*

CAPITOLUL II

Ei îți marchează cardul

Patronii magazinelor nu se bazează numai pe camerele de supraveghere pentru a afla diverse lucruri despre noi, în timp ce ne plimbăm printre rafturi sau ne plătim cumpărăturile la casele de marcat. Suntem participanţi benevoli la goana lor după informaţii, deoarece le oferim toate datele de care au nevoie pentru a construi un raport meticulos despre noi – şi o facem pentru nimica toată, an după an. Le permitem să îşi dea seama cum ne afectează publicitatea obiceiurile de cumpărători, cât de sensibili suntem la creşterea preţurilor, la ofertele cu reduceri, la lansarea unor noi produse şi la modul de aranjare a mărfurilor în magazine. Ei află dacă suntem bărbaţi sau femei, singuri sau într-o relaţie, tineri sau bătrâni, purtători ai unei sarcini sau deja părinţi, sportivi sau sedentari. Industria ne încurajează să ne vindem intimitatea pentru o reducere de 1%. Şi, pe măsură ce ne asamblează un portret detaliat în bazele lor de date, ei află mai multe despre noi decât ştie guvernul.

Mama mea a murit la o vârstă înaintată şi, după aceea, în timp ce îi umblam prin maldărele de obiecte personale şi îi scotoceam poşetele, am descoperit că avea în portofel şase carduri de fidelitate de la nişte supermarketuri. Ştiam că îi plăcea să le folosească. În ultimii ei ani de viaţă, o scoteam la cumpărături

la fiecare sfârşit de săptămână, deoarece, pentru ea, asta era o zi de vacanţă. După ce găsea fiecare lucru de pe lista ei de cumpărături şi porneam spre casa de marcat, fata de la tejghea o întreba dacă era „o membră a clubului“, iar mama mea făcea mare caz din a-şi căuta cardul şi a i-l înmâna. Accepta cardurile din două motive. Mai întâi, simţea că, dacă n-ar fi avut un card, ar fi pierdut ceva; în al doilea rând, îi plăcea să creadă că aparţine unui club. Nu a cerut niciodată vreuna dintre reducerile care i se cuveneau, din câte ştiu eu. Nici măcar nu cred că citea scrisorile pe care le primea de la magazin. Dar ea făcea parte dintr-o generaţie pentru care cumpătarea era o virtute, iar colecţionarea punctelor-bonus – un mod de a economisi bani, chiar dacă, de fapt, nu le solicita niciodată. Era datoria ei să fie prudentă. Atitudinea ei relaxată faţă de toate astea nu era reflectată de comercianţi, pe care i-a suţinut de-a lungul întregii sale vieţi.

La sfârşitul vieţii, fraţii şi surorile îi muriseră de mult şi avea doar familia apropiată şi îngrijitorii care să-i ţină de urât. Am descoperit că, timp de ani întregi, ea păstrase toate scrisorile primite, pe care le ţinea în cutii. Era, în cea mai mare parte, o colecţie deprimantă de corespondenţă bună de aruncat la gunoi, acceptări personalizate ale cererilor ei inexistente de carduri de platină „gratuite“, nenumărate oferte de împrumuturi, „sugestii folositoare“ de a face o ipotecă pe casă în schimbul unei croaziere în jurul lumii sau al unei noi sere şi multe altele de genul acesta. Săptămână după săptămână, an după an, ofertele au curs în valuri. Şi, desigur, au fost nenumăratele ocazii în care a câştigat „un premiu consistent în bani“. Tot ce trebuia să facă pentru a-l ridica, fără nici un fel de obligaţie, era „să sune la acest număr“. Mai jos, cu caractere mult prea mici pentru a putea fi văzute de ochii ei bătrâni, scria: „Apelurile se taxează cu cinci lire pe minut, pentru primele trei minute“. Nu a fost păcălită de nici una dintre aceste şarlatanii, deşi, în fiecare an, mii de femei bătrâne cad în capcană. În timp ce parcurgeam

mormane de oferte înzorzonate, m-am trezit întrebându-mă ce măsuri de protecţie există pentru cei bătrâni şi vulnerabili şi cine se ocupă de apărarea intimităţii lor.

Cine ştia unde locuieşte şi că era o proprietară în vârstă? Se ştia că nu avusese niciodată datorii, în lunga ei viaţă? În afară de familia ei apropiată, oamenii care ştiau cele mai multe lucruri despre ea erau patronii magazinelor pe care le vizita. Asta deoarece, cu ani în urmă, completase cereri pentru cardurile lor de loialitate şi, făcând asta, îşi divulgase toate datele personale. Continuase apoi să le dea informaţii, fără a avea nici cea mai vagă idee că ceea ce scrie pe formular avea să ajungă mai departe. Milioane de oameni pleacă urechea la sloganurile: „Fiecare mărunţiş contează", „Ştii că are sens", „Ai grijă de penny şi lirele vor avea singure grijă de ele", „Păstrează şi vei avea" sau „Paza bună trece primejdia rea". Doar una dintre aceste axiome moralizatoare nu e o rămăşiţă a înţelepciunii casnice victoriene, şi aceea e prima. „Fiecare mărunţiş contează" e, de fapt, un crâmpei isteţ de text publicitar, care defineşte filosofia cardului de loialitate al Clubului Comercianţilor, o extravaganţă de marketing şi de colectare de informaţii, pe care compania o descrie, grandios, drept un „întreg concept". Un „club de loialitate" standard din comerţ îmbrăţişează sentimentul călduros al apartenenţei la un club, ajutându-ne în acelaşi timp să economisim bani. O viaţă de cumpărături însumează sute de mici bonusuri, în special dacă mergem la acelaşi supermarket pentru tot ceea ce avem nevoie şi dacă putem răspunde „da" la toate întrebările sâcâitoare: „Aveţi un card de magazin Tesco / Safeway / Boots / Marks and Spencer / Target / Metro?", de fiecare dată când dăm o fugă să cumpărăm un kilogram de cârnaţi. Poate că îţi foloseşti cardul Nectar la Sainsbury's, Debenhams, BP şi Vodafone, caz în care aproape orice tranzacţie comercială pe care o vei efectua de-a lungul vieţii ar putea să îţi aducă

puncte. Şi ce înseamnă punctele? Simplu spus, PUNCTELE ÎNSEAMNĂ PREMII.

Desigur, nu e chiar aşa de simplu. Postează-te la casa de marcat din orice mare supermarket şi priveşte în jur. Acesta e un spaţiu amplu şi forfotitor, proiectat cu grijă pentru a deveni un colţ familiar şi prietenos al lumii tale. Alimentele sunt însumate pe bon şi achitate, poate, cu cardul tău Visa. Fidelitatea îţi e recunoscută cu o trecere a cardului peste senzor şi cu un zâmbet din partea fetei de la casă, apoi îţi împingi căruciorul cu produse cumpărate spre maşină, pe lângă agentul de securitate şi pe lângă senzorii antifurt. Nu vrei să ştii că undeva, deasupra ta, tranzacţia a fost filmată prin televiziunea digitală cu circuit închis, plata a fost înregistrată şi cronometrată, iar imaginea trupului şi a feţei tale au fost înregistrate în baza de date, cu detalii despre cardul de loialitate. Magazinul deţine acum aspecte ale identităţii tale care ar face orice poliţist din serviciile secrete să rânjească invidios.

Cardurile de fidelitate sunt forma rafinată şi modernă a timbrelor Green Shield, un sistem de a economisi bani lansat prin anii 1950. În acest sistem, primeai timbre Green Shield ori de câte ori făceai o achiziţie şi le lipeai într-un album, până când aveai suficiente pentru a le răscumpăra. Cu cât economiseai mai mult, cu atât mai mare era recompensa. Timbrele Green Shield erau bune, deoarece te învăţau să faci economii şi să fii cumpătat, şi erau reconfortante, deoarece, pe atunci, colecţionarea timbrelor era un hobby popular, pe care toată lumea îl înţelegea. Colecţionarea timbrelor era un lucru bun şi pentru Green Shield, pentru că îşi vindeau micile timbre supermarketurilor şi ofereau recompensele. Problema cu timbrele Green Shield era că, pe atunci, comercianţii obţineau foarte puţin din vânzări, în afara loialităţii clienţilor, şi cu toţii ştim că nu există cadouri pe degeaba. În cele din urmă, negustorilor de alimente le-a picat fisa că puteau economisi bani răsplătind chiar ei loialitatea

clienților și îngropând cheltuielile în bugetul de marketing. După care și-au dat seama că nu doar vor economisi bani, dar, ci și că prin înregistrarea tranzacțiilor într-un computer central, vor construi o bază de date cu preferințele de cumpărare ale clienților, care va deveni, cu trecerea timpului, o resursă neprețuită.

Conceptul de carduri de fidelitate pare foarte generos. Întreprinderea îți obține loialitatea, iar tu îți primești punctele, milele aeriene sau voucherele. Din păcate, e puțin mai complicat de atât. Dacă, de exemplu, te muți în comitatele din jurul Londrei și mergi la cumpărături la Shopco de trei ori pe săptămână, ți se va aduce mereu la cunoștință că deținerea unui card al clubului te va copleși cu beneficii din belșug. Nu te vei putea abține să nu intri în club și vei căpăta, curând, obiceiul de a prezenta cardul de fiecare dată când mergi la cumpărături. Fiecare casă de marcat din fiecare magazin este conectată la baza de date a clubului, iar rezultatul e că fiecare coș cu provizii pe care îl cumperi este înregistrat și cercetat, până când se va fi construit o imagine detaliată asupra ta. Dacă ți s-ar prezenta această analiză a ta, după câțiva ani de „loialitate“, ar fi posibil să ți se pară alarmantă, dacă nu defăimătoare. Dar nu poți face mare lucru. Tipii în costume din clădirile opace de birouri ale cartierului general transformă faptele indiscutabile, spicuite din coșurile tale de cumpărături, în carnea și oasele propriilor creații. În ceea ce-i privește, ești ceea ce cumperi, iar profilul pe care îl creează, pe baza cardului tău, este precis până la ultimul cub de bulion.

Când depui cererea pentru cardul lor de loialitate, ți se dă un „Acord“ care garantează că datele tale private sunt în siguranță la Shopco. De asemenea, ți se promite că, dacă precizezi că nu vrei să fii contactat pentru studii de piață, nu te vor deranja. Ei mai afirmă că se supun Legii protecției datelor (ceea ce, oricum, reprezintă o obligație prevăzută prin lege). Formularul tău de cerere presupune să completezi detaliile personale,

inclusiv numele, adresa, vârsta ta şi a tuturor celor care trăiesc la aceeaşi adresă. Mai trebuie să completezi şi detalii legate de gospodărie, necesităţi dietetice şi informaţii de contact, inclusiv adresa de e-mail, numărul de telefon mobil ş.a.m.d.

În schimb, ţi se va trimite un card care îţi va permite să câştigi un punct pentru fiecare liră sterlină cheltuită în magazin şi vei putea să profiţi de oferte speciale pentru noi linii de produse, plus puncte de bonus. Cumpără „online" şi vei face economii chiar mai mari. Fiecare punct pe care îl câştigi valorează un penny sau 1% şi poţi alege să îţi ridici recompensele imediat ce acestea devin disponibile sau ori de câte ori te hotărăşti să le încasezi. Poţi să le laşi să se adune ani întregi, dacă aşa ai chef. Sunt oameni înregistraţi în bazele de date ale supermarketurilor cu mii de lire sterline, adunate sub forma punctelor de recompensă care li se datorează. Care-i clenciul? Punctele nu stârnesc interes. În baza de date a corporaţiei American Express există cecuri de călătorie emise, încă nefolosite la ani buni după ce vacanţa pentru care au fost eliberate a devenit de mult doar o amintire îndepărtată. Din punctul de vedere al AmEx, acesta e un lucru nepreţuit. Cecurile de călătorie, în sine, nu aduc profit, în timp ce banii plătiţi pentru ele sunt investiţi de AmEx şi aduc beneficii de 6% sau chiar mai mult.

Nu eşti obligat, însă ar trebui să câştigi 150 de puncte ale clubului Shopco în timpul fiecărei perioade de colectare, care durează, fiecare separat, cam trei luni. Cardul încurajează şi glorifică fidelitatea, ceea ce e un lucru bun pentru Shopco şi îl face pe client să se simtă bine faţă de sine însuşi şi liniştit că magazinul este un element sigur, demn de încredere şi prietenos în viaţa sa. Ia-ţi un card şi, de-a lungul anilor, informaţia pe care acest mic petic de plastic o transmite, codat, la Shopco, prin intermediul tejghelei şi prin baza de date, devine spionul din portofelul tău, care înregistrează cum îţi trăieşti viaţa şi trage concluzii pe baza obiceiurilor tale de cumpărător. Nu le va spune

analiştilor din cartierul general Shopco din Hertfordshire doar că ai un animal de companie, porţi proteză dentară sau suferi de flatulenţă. Aplicând nişte programe socio-demografice complicate la stilul tău de viaţă şi la cel al altor 20 de milioane de clienţi, ei vor fi în stare să stabilească stadiul existenţei pe care tu – şi alţii din gospodăria ta – l-aţi atins. Stilul tău de viaţă va influenţa tot soiul de produse vândute prin cele 3 000 de magazine ale Shopco. Obiceiurile tale de cumpărător vor fi transmise celor care produc mâncarea animalului tău de companie, adezivul tău pentru proteză şi ceainicul tău electric. Pornind de aici, Shopco va face presupuneri despre mărimea venitului tău, despre pasiuni şi preocupări, despre ceea ce obişnuieşti să bei, despre atitudinea ta faţă de viaţa sănătoasă, despre activitatea ta sexuală, despre nivelul de educaţie şi despre surplusul de venit, şi îţi va stabili poziţia pe firmamentul socio-economic potrivit tehnicienilor de la cartierul general Shopco Megacorp. Vor şti când îţi schimbi domiciliul, când mergi în vacanţă, când eşti bolnav şi când vei avea un copil.

Dar asta e încă în regulă. Până la urmă, sunt doar simpli băcani şi tot ceea ce urmăresc sunt banii. Sau nu e aşa? Când te muţi şi-ţi schimbi adresa de pe card, sunt mari şanse să primeşti un mic dar cu vouchere alese în mod special pentru un nou proprietar de casă (poate nişte produse de curăţat), împreună cu o listă de adrese şi de numere de telefon ale magazinelor locale. Nivelul generozităţii va corespunde statutului tău în baza de date. În ceea ce priveşte descoperirea că a sosit un nou copil, ronţăitorii de cifre vor ajunge să-şi dea seama de acest lucru din modul în care îţi modifici profilul cumpărăturilor. Brusc, scutecele de unică folosinţă şi laptele praf vor apărea drept achiziţii regulate în baza ta de date. Poate că te vor invita să intri în Clubul Sugarilor din compania lor? Sună, într-adevăr, foarte fermecător, în lumina asta. Industria de retail deţine, în prezent, vaste cantităţi de informaţii de acest gen despre noi.

Pretextând că vor să-şi îmbunătăţească randamentul şi serviciile pe care le oferă clienţilor, comercianţii au creat bănci de informaţii care s-ar dovedi nepreţuite pentru tot felul de grupuri, inclusiv pentru multe cărora, mai mult ca sigur, nu ai dori să le împărtăşeşti detaliile personale. Problema, în acest caz, este că nu vorbim despre date bancare. Sunt detalii ale clienţilor adunate de comercianţi. Dacă un băcan observă că poate profita de pe urma unor resurse precum datele cardului de loialitate, va fi tentat să o facă. Dar cine ştie unde ar putea ajunge aceste informaţii? Supermarketurile americane au oferit, de bunăvoie, FBI-ului amănuntele despre cardurile lor de fidelitate, după 9/11. Acceptabil, s-ar putea spune – aceea a fost, într-adevăr, o situaţie de criză. Da, dar a fost şi începutul unei afaceri foarte grase. A înlesnit transmiterea datelor spre politicieni pe care s-ar putea să nu-i sprijini şi care nu ai vrea să-ţi cunoască detaliile personale. Clienţilor din bazele de date ale supermarketurilor nu li s-a spus niciodată că informaţii despre ei au fost oferite guvernului. A fost un ajutor inestimabil pentru autorităţile federale, care erau în curs de a crea o formulă de spionaj capabilă să-i ajute să identifice posibilele ameninţări teroriste. În perioada care a urmat catastrofei, agenţii FBI au studiat tranzacţiile cu cardurile de loialitate ale atacatorilor, în încercarea lor de a crea profiluri ale obiceiurilor de consumatori ale acestora.

O bună parte din arsenalul politicianului modern e exat pe identificarea grupurilor-ţintă – exact ceea ce încearcă să facă cluburile de loialitate. Rapoarte recente, publicate în Marea Britanie şi în Statele Unite, sugerează că transmiterea acestor date către terţi se întâmplă mai des decât ar vrea cei din industria de retail să ne facă să credem. În Marea Britanie, Partidul Conservator a pus la punct „Trezorerii electorale", în timp ce Partidul Laburist are baze de date similare, numite „Contacte laburiste". Votanţii sunt împărţiţi în diferite grupuri diferenţiate după criterii socio-economice, cum ar fi maşina pe care o

conduc, codul poştal sau unde şi de câte ori pleacă în vacanţă. Informaţiile permit partidelor să ne anticipeze intenţiile de vot, ceea ce, mai departe, le ajută să se hotărască asupra mesajului pe care ni-l vor adresa. Contactul direct cu electoratul, prin intermediul e-mailurilor personalizate şi al campaniilor telefonice, e o tehnică ce a fost rafinată, în Statele Unite, cu un succes uluitor de către directorul de campanie a lui George Bush, Karl Rove. Acesta a folosit 300 000 de voluntari într-o campanie de marketing multistratificată, utilizând informaţii precise pentru a se adresa votanţilor, circumscripţie cu circumscripţie. În timpul ultimelor trei zile ale campaniei, voluntarii pentru echipa Bush / Cheney au trimis e-mailuri la 7,2 milioane de votanţi. Multe dintre informaţiile pe care le-au folosit proveneau din bazele de date ale cardurilor de fidelitate. O abordare similară a fost adoptată în 2005 de toate cele trei partide participante la alegerile generale din Marea Britanie.

Australianul Lynton Crosby, cel care l-a ajutat pe John Howard să adune patru victorii consecutive în Australia, a folosit sistemul Mozaic de clasificare, pus la punct de Experian (compania de evaluare a creditelor şi de date ale consumatorilor) în timpul campaniei din 2005 a Partidului Conservator. Sistemul împarte populaţia în 61 de categorii şi 11 grupări. Lista votanţilor folosită de conservatori şi laburişti se baza, în parte, pe referendumul din 2001 şi, în parte, pe informaţii din sondajele în rândul consumatorilor şi pe înregistrări ale cheltuielilor luate din bazele de date ale cardurilor de fidelitate.

Analistul de baze de date Joe Patel, care scrie pentru *Atlanta Constitution,* a afirmat că magazinele vând şi folosesc ca monedă de schimb, în mod regulat, bazele de date care înregistrează preferinţele clienţilor, compilate din mereu popularele carduri cu reduceri pentru cumpărături. *Media Week* a susţinut că Tesco, Thomas Pink, MCV şi New Look şi-au scos, toate, la vânzare informaţiile despre clienţi, pentru alte companii de marketing.

Caspian Group, care militează împotriva sistemelor cu carduri de fidelitate, afirmă că datele culese de pe carduri sunt folosite, în mod regulat, în tribunalele britanice şi americane. Detaliile despre vânzări pot fi stocate alături de imagini filmate ale posesorilor de carduri. Caspian susţine că s-a înregistrat o creştere a cazurilor de cumpărători care au dat de bucluc din cauza unor greşeli făcute de analiştii care le-au studiat datele. Cu atâtea informaţii adunate şi cu atâtea întrebuinţări care se găsesc pentru ele în fiecare zi, astfel de probleme sunt inevitabile, iar abuzurile vor începe să se strecoare în sistem.

Deja există cazuri de analişti care au modificat programul ca să permită accesări ilegale. O femeie din Milton Keynes a fost arestată, iar casa i-a fost percheziţionată de poliţişti, după ce a fost filmată, pe un sistem de televiziune cu circuit închis dintr-un supermarket, în timp ce-şi introducea în poşetă propria eşarfă. Paza magazinului a crezut că furase eşarfa şi a identificat-o prin datele cardului ei de loialitate. Deşi e foarte dificil, dacă nu chiar imposibil, să elimini toate riscurile unor asemenea incidente, care au legătură cu toate companiile cu care interacţionezi, poţi să îţi micşorezi implicarea în programe acolo unde nu e obligatoriu să oferi informaţii personale. Şi ţine minte: chiar dacă foloseşti o identitate „falsă“ la supermarketul din zona ta, imediat ce scrii un cec sau foloseşti o carte de credit, ei pot pune în legătură acea informaţie cu profilul tău „fals“.

De fapt, nu datele sunt problema, ci oamenii pe mâinile cărora ajung ele. Avem de-a face cu o industrie care tolerează concepte precum „Wizmark“ – un ecran de 8,5 cm, care e plasat în pisoare şi activat de mişcarea lichidului. Curgerea declanşează un afişaj cu lumini pâlpâitoare, însoţite de un mesaj publicitar. Când e vorba de marketingul pentru industria de retail, orice e permis.

Riscul invadării intimităţii a crescut, în mod dramatic, odată cu introducerea identificării prin frecvenţe radio (RFID) pentru

o lungă listă de produse. Sistemul folosește cipuri minuscule de calculator, mai mici decât un grăunte de nisip, pentru a urmări mărfurile la distanță. Sunt cunoscute drept „cipuri-spion“ și au fost ascunse în ambalajele multor produse – cum sunt lamele de bărbierit Gillette – pe care le puteți cumpăra la supermarket. Fiecare cip e pus în legătură cu o antenă, care captează energia electromagnetică emisă de un dispozitiv de citire. Când detectează energia, cipul răspunde trimițând un număr de identificare unic lectorului, ceea ce permite identificarea obiectului. „Cipul-spion“ poate transmite informații de la câțiva centimetri până la 30 de metri depărtare. Tehnologia e disponibilă din 1999 și toți marii comercianți din Marea Britanie au efectuat teste de fezabilitate pentru sistem. Dacă nu va apărea o rezistență organizată și zgomotoasă a consumatorilor, ei vor marca, în cele din urmă, fiecare obiect fabricat pe Pământ cu acest sistem, ca înlocuitor pentru codul de bare. Tesco, Procter and Gamble, Gillette și Wal-Mart au făcut, toți, experiențe în acest sens. Testele din Marea Britanie au fost, parțial, finanțate de Ministerul de Interne – un gest politic ce va fi, fără îndoială, scos din nou la iveală în viitor, când industria de retail va fi, în cele din urmă, trasă la răspundere.

În cel mai bun caz, tehnologia RFID ajută la urmărirea mărfurilor de la producător la depozit și apoi în magazin. Ar putea fi folosită la recuperarea unor comenzi pierdute sau la alertarea echipei de securitate, atunci când un produs este furat. Într-un viitor nu prea îndepărtat, producătorii de bunuri pentru gospodărie ar putea veni din urmă creând, de exemplu, o tehnologie care să îți spună cum să prăjești o rață congelată pe care tocmai ai cumpărat-o sau cum să faci un sos gustos. Opoziția față de RFID se bazează pe protejarea intimității. Cu un cod de bare standard, un produs precum o cutie de cola dietetică are un cod de produs universal, identic pentru toate cutiile de tipul respectiv. Dacă acest cod de bare ar fi înlocuit de RFID, fiecare cutie ar

avea un număr de identitate unic. Acesta ar putea fi pus în legătură cu clientul care a cumpărat-o, respectivul putând fi identificat atunci când un card de credit sau de loialitate e scanat la tejghea. Aşadar, dacă mergi la Shopco şi cumperi o sticlă de Head & Shoulders care e marcată cu RFID, plătind cu un card Visa şi solicitându-ţi punctele de pe un card de fidelitate, vei fi, iremediabil, pus în legătură cu acea sticlă de şampon (şi cu faptul că ai mătreaţă). Comercianţii aduc argumentul că raza de identificare a cipurilor e foarte scurtă. Acest fapt nu e adevărat, deoarece cipurile pot fi citite la distanţă, cu un echipament mai sofisticat. Nu numai atât: ele pot fi, de asemenea, citite în portofelul sau în poşeta ta şi prin haine, fără să ai habar de asta. Nu e nevoie decât de aparatul de citire potrivit. Ceea ce înseamnă că, atunci când eşti pus în legătură cu un produs marcat, un străin poate să îndrepte un aparat de citire ascuns spre tine, pentru a afla conţinutul genţii sau al servietei pe care o porţi şi ce ai în buzunare, fără ca tu să-ţi dai seama de nimic.

Când se va utiliza pe scară largă în Marea Britanie, tehnologia va permite sistemului să ne urmărească mişcările 24 de ore din 24. Dacă industria de retail va pune în aplicare ceea ce intenţionează, vor exista cipuri şi cititoare RFID pretutindeni. Ele vor fi ascunse sub duşumele, în avioane, magazine, frigidere şi hoteluri. Nu numai că ne vom pierde intimitatea, dar vom fi bombardaţi permanent cu energie electromagnetică. Tehnologia a evoluat rapid şi în prezent e posibil să „imprimi" cipurile-spion. Ceea ce înseamnă că un punct de pe o pagină tipărită sau de pe o bucată de plastic poate fi folosit pentru a lua urma cuiva. Antenele pot fi, şi ele, imprimate, făcând astfel cipurile-spion practic invizibile.

Tehnologiei, dezvoltate iniţial în Japonia, i se minimalizează în prezent importanţa, comercianţii susţinând că e vorba de un simplu „cod de bare radio". A fost adoptată ca o alternativă la codurile de bare normale, care nu sunt considerate sigure şi care

fac, tot mai des, obiectul unor escrocherii. Probabila trecere a comercianţilor la RFID a alarmat grupurile de presiune, care sunt conştiente că cipurile pot fi citite, de la mare depărtare, de dispozitive din afara magazinelor. Grupurile care luptă pentru drepturile cetăţenilor şi ale consumatorului au încercat să impună un boicot mondial, de exemplu împotriva magazinelor Shopco, deoarece ele au extins perioada de testare a sistemului. Protestatarii consideră că cipurile RFID ar trebui menţinute în interiorul depozitului şi al lanţului logistic, şi nu ar trebui să li se permită contaminarea infospaţiului cu poluanţi care corodează intimitatea, dincolo de casele de marcat. Potrivit Grupului Caspian, RFID este prea rudimentar, din punct de vedere electronic, pentru a permite încorporarea unei tehnologii de criptare ce ar putea oferi nişte garanţii de protecţie. Pentru a înrăutăţi lucrurile, cipurile-spion nu pot fi „ucise" (anulate) la casa de marcat şi, astfel, continuă să funcţioneze la nesfârşit. Shopco şi-a extins perioada de probă de 12 luni de la două magazine la zece şi a comandat 4 000 de cititoare RFID şi 16 000 de antene pentru incendii şi de protecţie de la compania ATD Security Services. Marks and Spencer a efectuat un test la şase dintre magazinele lanţului, în 2004. În timpul testului, clienţii M&S nu au fost avertizaţi că achiziţionează bunuri marcate.

Probabil singurele inconveniente ale cipurilor RFID vor fi costul şi legislaţia. Tehnologia e costisitoare, menţinându-se în prezent la puţin peste 15 penny bucata. Acest lucru adaugă un surplus destul de simţitor, să spunem, unei cutii de cola dietetică, şi e foarte probabil ca preţul să rămână ridicat în viitorul apropiat. De asemenea, e posibil ca cipurile RFID să contravină Legii protecţiei datelor din Marea Britanie şi legislaţiei europene cu privire la drepturile omului. E sigur că aceste sisteme vor fi puse la încercare la tribunal, atât în Statele Unite, cât şi în Europa. În Germania, reţeaua de supermarketuri Metro a inclus RFID în sistemul lor de carduri de loialitate şi şi-a

justificat gestul prin faptul că acest lucru le-a permis să verifice vârsta cumpărătorilor care doreau să vadă filmuleţele promoţionale ale unor DVD-uri pentru adulţi. Informaţiile despre cumpărător erau stocate într-o bază de date, conectată printr-o reţea wireless la un cititor RFID din secţiunea de DVD-uri a magazinului. În cele din urmă, Metro a abandonat testul, ca urmare a protestelor clienţilor. „Ne vom întoarce la codurile de bare", au declarat ei. Totuşi, au continuat prin a comenta că nici una dintre celelalte zone în care Metro foloseşte tehnologia RFID nu va fi afectată de această decizie. „Suntem decişi să folosim RFID în managementul reţelei de aprovizionare." Magazinul cere, în prezent, celor mai mulţi dintre furnizorii săi să ataşeze cipurile inteligente paleţilor şi ambalajelor de transport. Comerciantul american Target a impus o condiţie similară furnizorilor săi locali, începând cu 2005. E doar o chestiune de timp până când sisteme asemănătoare vor fi folosite în Marea Britanie.

Tehnologia RFID se află încă la început, dar va deveni curând un lucru obişnuit în vieţile noastre. Este acceptată, la scară foarte largă, în Statele Unite, unde e folosită în industria jocurilor de noroc. Acolo, cipurile sunt încastrate în jetoanele de joc, ca mijloc de a reduce frauda şi de a-i supraveghea pe marii jucători. Cazinourile britanice au examinat şi ele sistemul, dar până acum au refuzat să-l întrebuinţeze, invocând costurile şi necesitatea sa redusă (ar fi ca şi cum ai lua un baros pentru a sparge o nucă, au zis ei). Studenţi de la universităţi din toată America sunt monitorizaţi prin intermediul cardurilor pe care le poartă, în care este inclus cipul. Când ajung la şcoală dimineaţa, RFID activează un ecran pentru a le înregistra sosirea şi le afişează fotografia. Este eliminată astfel metoda manuală, mai veche, de a ţine un catalog de prezenţă. Astăzi, în loc să marcheze numele studenţilor pe o planşetă, sistemul este computerizat. Şcolile şi colegiile care îl folosesc spun că fac acest lucru pentru a implementa o securitate mai bună, un management al timpului ameliorat şi

o eficienţă mai mare. Zece inspectorate şcolare locale din Marea Britanie testează o idee similară. Este acelaşi sistem folosit pentru a-i urmări pe infractori englezi aflaţi în arest la domiciliu sau sub diverse interdicţii de circulaţie, pe deţinuţii din penitenciarele din Texas şi pe prizonierii irakieni de război. IBM a anunţat că intenţionează să includă etichete electronice în cărţile de credit şi în carnetele de cecuri.

După relaxarea reglementărilor de carantină antirabică pentru animalele din Europa, animalele pot fi inoculate, iar tratamentul poate fi înregistrat pe un cip electronic implantat în gâtul acestora. Multe mii de animale din Marea Britanie sunt marcate în acest fel, iar cipul îi ajută, de asemenea, pe angajaţii de la Protecţia Animalelor să urmărească şi să identifice exemplarele abandonate. Pentru americani a devenit un lucru obişnuit şi, în unele locuri, la modă să aibă cipuri implantate în propriul corp. Companiile din Florida care utilizează tehnologia promovează deja această simplă operaţie cu argumentul că părinţii şi cei care au grijă de copii îi pot supraveghea astfel pe micuţi. În 2004, o companie de securitate numită Metrorisk a implantat cipuri numite VeriChips Procurorului General al Mexicului şi altor zeci de colegi sau membri ai echipei sale. Cipul le permite accesul rapid în clădiri şi săli de judecată protejate, fără a mai purta carduri de identitate. E adevărat că, atunci când vine vorba despre a ieşi, într-un fel sau altul, în evidenţă, americanii au tendinţa de a fi mai puţin inhibaţi decât cetăţenii altor ţări, care ar putea să considere inacceptabilă implantarea unor cipuri de identitate în corpul lor, ca un procedeu ce permite economisirea de timp şi de muncă. Tehnologia există şi în Marea Britanie. Putem fi marcaţi, în mod discret, de chirurgii plasticieni de pe Harley Street. Totuşi, aceasta tinde să fie o practică pe care englezii o ţin secretă.

Utilizarea sistemelor de urmărire poate administra o lovitură mortală libertăţilor fundamentale. Grupul pentru drepturi

cetăţeneşti Liberty, cu sediul în Marea Britanie, susţine că autoritatea asupra sistemului nu ar trebui lăsată companiilor comerciale, companiilor de securitate sau avocaţilor şi contabililor particulari, atenţionând că guvernul nu a elaborat încă nici un proiect de lege pentru reglementarea informaţiilor generate de RFID. Tehnologia este foarte adaptabilă. Abonamentul folosit pentru metroul londonez o utilizează de peste doi ani. Cardul de transport are numele şi adresa deţinătorului şi trimite informaţii ori de câte ori este scanat, la începutul şi la sfârşitul călătoriei. Conform Autorităţii de Transport londoneze, datele vor fi păstrate „pentru o vreme". Dacă îţi plăteşti călătoria cu un card de credit sau de debit, aşa cum fac multe persoane, traseele tale prin Londra vor fi înregistrate cu o precizie milimetrică. Toate maşinile britanice şi europene au început să fie dotate cu dispozitive de urmărire începând din 2005 şi poţi cumpăra deja telefoane mobile cu astfel de dispozitive ataşate. Banca Centrală Europeană a încorporat etichete electronice în toate bancnotele euro, iar Banca Americii studiază un cip produs de compania japoneză Hitachi, cu perspectiva de a marca bancnotele americane.

În urmă cu 30 de ani, pe lângă mai sus-amintita previziune despre puterea de procesare a computerelor, care se va dubla la fiecare 12 luni, fondatorul companiei Intel, Gordon Moore, a spus că orice dispozitiv sau sistem care foloseşte microcipuri va deveni rapid mai mic, mai mobil, mai eficient şi mai puţin costisitor. Previziunea lui Moore se aplică, în egală măsură, internetului, care este construit din sisteme ce sparg datele în „pachete" sau în fragmente, le distribuie către destinaţiile corecte şi le reasamblează, la intervale de nanosecunde. Sistemul, cunoscut drept TCP/IP, a fost capabil să absoarbă o gamă largă de tehnologii pe lângă comunicaţiile prin internet, inclusiv site-urile şi serviciile de telefonie mobilă. Nu mai e mult până când telefoanele noastre, laptopurile, pagerele – de fapt, toate

dispozitivele noastre de comunicare – îşi vor uni forţele pentru a crea cel mai masiv sistem de supraveghere conceput vreodată. Zilele tranzacţiilor în numerar se apropie de sfârşit şi fiecare achiziţie va deveni un bit de informaţie înregistrat pe un hard disk şi asociat, direct, cu detaliile personale ale individului implicat. Înregistrarea va dăinui până când discul va fi distrus.

Cardurile de fidelitate şi dispozitivele de urmărire vor oferi întreprinderilor private mai multe informaţii personale despre bărbaţii şi femeile de rând decât posedă, în clipa de faţă, cel mai tiranic dintre statele poliţieneşti. Merită avantajele pe care le obţinem din acest tip de săpare a datelor şi din această tehnologie riscul pe care ni-l asumăm? Industria de retail şi producătorii sistemelor RFID au susţinut cu convingere că adunarea informaţiilor despre tiparele de cumpărare este un procedeu demn de admiraţie, care aduce beneficii tuturor şi care nu are nimic de-a face cu monitorizarea membrilor individuali ai publicului larg. Dar e sigur că vom putea să alegem să ieşim din sisteme care ne îngrijorează? Ce fel de protecţie există pentru informaţiile pe care aceste organizaţii le-au strâns în legătură cu noi? Acţiuni înregistrate pe cardurile de loialitate au fost deja folosite ca dovezi în tribunale. Puţini dintre noi îi abordează pe comercianţi pentru a-şi exprima îngrijorarea în legătură cu confidenţialitatea şi cu informaţiile private pe care le adună despre noi. Tehnologia RFID va fi implementată, orice am face noi. Cardurile de loialitate au devenit o parte a vieţii cotidiene. Singura metodă de a ne proteja pe care o avem la îndemână este să aruncăm cardurile de fidelitate şi să plătim în numerar.

Capitolul III

Avem numărul dumneavoastră. Și numele...

Obţinerea rapidă şi fără costuri suplimentare mari a unui credit a devenit un lucru obişnuit. Poţi obţine o ipotecă printr-o simplă convorbire telefonică. Nu va trebui să furnizezi prea multe date, numele şi adresa vor fi de ajuns. După răspunsul la întrebarea dacă eşti proprietarul apartamentului în care locuieşti, vei primi un „Da" sau un „Nu" cât ai zice peşte. În câteva secunde doar, poate fi vizualizat scoringul tău de credit, accesând una dintre cele 12 uriaşe baze de date naţionale aparţinând unor companii precum Experian sau Equifax. Companiile de creditare şi de ipotecare au contracte cu tot soiul de firme de acordare a scoringurilor şi se folosesc de acestea fără prea mari mustrări de conştiinţă, pentru a-şi forma o opinie pentru fiecare cerere primită. Problemele încep atunci când sistemul dă greş. Companiile de consultanţă pentru acordarea creditelor sapă după informaţii financiare ale persoanelor, le includ în bazele lor de date, pe care apoi le vând. Aceste companii ajung să ştie fiecare situaţie în care ai întârziat la plata unui împrumut. Sistemul nu este infailibil: datele pot proveni din surse îndoielnice, iar greşeli se pot face oricând. Corectarea acestor erori este, însă, o chestiune de noroc, pentru că aceia care acordă scoringuri nu vor niciodată să rişte. Ei preferă să lase

listele așa cum sunt și nu sunt dispuși să-și asume riscul de a gira un solicitant care să se dovedească apoi incapabil de a-și îndeplini obligațiile.

Zeci de companii vând astfel de informații personale. Nici o instanță de creditare care se respectă nu își va furniza serviciile cuiva înainte de a fi consultat una dintre multele agenții de acordare a scoringurilor, care a tot strâns astfel de informații despre tine de-a lungul întregii tale vieți ca adult. La urma urmei, banii acordați cu împrumut trebuie justificați în fața acționarilor sau a șefului. Simplificând, fiecărui adult îi corespunde un fișier cuprinzător, în care sunt înscrise toate elementele ce pot prezenta fie și o minimă relevanță în privința calității sale de potențial debitor. Informațiile incluse în fișier sunt cumpărate sau obținute din arhive publice – precum cele ale tribunalelor, ale Protecției Sociale sau ale Oficiului de Cadastru – ori private (neachitarea la timp a obligațiilor ce privesc cărțile de credit, creditele bancare sau leasingurile). Profilul persoanei este înscris într-o bază de date, iar apoi pus la dispoziția abonaților sau a oricui are nevoie de aceste informații și este dispus să plătească pentru ele.

Scoringurile sunt utilizate de poliție și de serviciile secrete pentru a construi profiluri ale persoanelor implicate în investigațiile în derulare. Unele date sunt mai prețioase decât altele. Se poate dovedi dificilă inițiativa de a achiziționa informații privind o persoană sau un grup care posedă un statut aparte. În Marea Britanie, conform Legii protecției datelor, dosarul personal trebuie arătat, la cerere, subiectului său. Și totuși, chiar și în acest caz, companiilor li se permite să perceapă un tarif pentru că-ți trimit elemente din propriul dosar.

Experian este una din cele mai mari companii britanice de acordare a scoringurilor. Compania poate informa un potențial creditor dacă un solicitant a declarat vreodată faliment, dacă a fost nevoit să cadă la înțelegere cu alți creditori, dacă a scris

vreodată cecuri neacoperite, dacă a sărit o rată, de orice fel ar fi aceasta, sau dacă a fost cândva condamnat pentru fraudă. Când şi când, poate oferi alt tip de informaţie utilă creditorilor, precum numărul de înregistrare la Protecţia Socială sau numărul de înmatriculare al maşinii, de câte ori solicitantul a încălcat Codul Rutier sau dacă şi-a schimbat cu regularitate furnizorul de cărţi de credit, pentru a beneficia de o dobândă mai bună. Banca sau furnizorul de credit abonat plăteşte pentru datele primite şi are tendinţa să le trateze ca literă de lege. Acordarea creditelor este o afacere de amploare şi cei care dau bani cu împrumut nu sunt foarte flexibili în ceea ce fac. Nu există excepţii de la regulă.

Datele de eligibilitate la solicitarea creditelor nu reprezintă singurul gen de informaţie disponibilă pe piaţă. Profilurile psihologice ale angajaţilor sunt cumpărate în mod curent de către agenţiile de recrutare şi de către instituţiile publice, inclusiv de cele de învăţământ sau de menţinere a ordinii publice. În Marea Britanie, unde „pedofilul răpitor" a devenit sperietoarea publică cu cea mai mare vizibilitate, reguli foarte restrictive stabilesc cine este şi cine nu este potrivit pentru a lucra cu copii. Tuturor profesorilor şi angajaţilor din învăţământ li se verifică minuţios trecutul profesional, precum şi alte înregistrări despre ei, înainte de a li se permite să înceapă lucrul. Chiar şi jucătorii de golf profesionişti, instructorii de înot sau de cercetaşi trebuie să aibă dosare ireproşabile pentru a li se permite să-i înveţe pe copii. Iar responsabilitatea de a se asigura că toţi membrii personalului sunt dincolo de orice suspiciune, înainte ca aceştia să înceapă lucrul, le revine angajatorilor.

Furnizorilor de date li se cere în mod frecvent să ofere informaţii de bază. Dacă ele sunt eronate, îi pot stigmatiza pe cei la care se referă. Dacă persoana care a fost nedreptăţită doreşte să se adreseze justiţiei, unica sa opţiune este de a recurge la legile civile ale defăimării – pentru care, în Marea Britanie, rareori se

poate oferi consiliere juridică. El sau ea ar mai putea invoca Legea drepturilor omului sau s-ar putea adresa Curții Europene, dar, indiferent unde ar căuta reparație legală, are în față un proces lung și care îi va pune serios nervii la încercare. În Statele Unite există legi care le protejează pe victimele informațiilor inexacte. Cea mai importantă este Legea raportării corecte a datelor necesare obținerii creditelor (1970), care reglementează accesul la date și dreptul de a corecta inexactitățile. Și cam atât.

Din păcate, agențiile de acordare a scoringului și alte companii care manevrează informații de ordin personal sunt recunoscute pentru obiceiul lor de a furniza date inexacte. Pentru aceasta pot exista două motive: fie au primit, la rândul lor, informații incorecte, fie aceste informații sunt corecte, dar au fost introduse greșit în baza de date. Deși Legea protecției și Legea libertății informațiilor din Marea Britanie garantează accesul la date, acestea nu asigură în același timp și aducerea la zi sau corectarea în timp util a bazelor de date, atunci când se descoperă inadvertențe. În industria informațiilor nerespectarea drepturilor cetățenești frizează aroganța. Situațiile în care mai multe persoane au descoperit că fuseseră clasificate, în mod eronat, ca fiind necinstite sau că înregistrările privind activitățile și caracterul lor fuseseră alocate altei persoane ori erau pur și simplu răuvoitoare sunt deja banale.

Multe persoane vârstnice sunt puse în situații jenante de agențiile de obținere a informațiilor financiare. Companiile furnizoare de cărți de credit refuză adesea efectuarea tranzacțiilor, fie și din motivul că utilizatorul nu și-a folosit cardul de ceva vreme. În momentul achitării cumpărăturilor, furnizarea de lichidități este refuzată automat, cu toate neplăcerile ce decurg din aceasta. Există multe situații în care coeficientul cuiva poate avea de suferit din cauze neimputabile lui. Exemplul tipic este acela al diferendului legal dintre bancă și client pe marginea

unui împrumut neachitat. Clientul poate crede cu tărie că are dreptate. În mod cu totul arbitrar, banca decide să lase rezolvarea disputei pe mâinile unei agenţii de recuperare a debitelor şi să paseze informaţiile unor companii precum Experian sau Equifax. Clientul poate să meargă până în pânzele albe cu contestarea datoriei, astfel încât primii recuperatori de debite pot vinde „datoria" acestuia altei firme, încă şi mai lipsite de scrupule. Aşa-zisul debitor, sătul, în cele din urmă, de această neîntreruptă hărţuire şi dorind pur şi simplu să rezolve până la urmă problema, decide să plătească acestui al doilea recuperator. Chiar şi aşa, banca clientului a înregistrat acum împrumutul şi refuză ştergerea din evidenţe a întârzierii plăţii, pe motiv că nu deţine nici o dovadă că aceasta a fost în cele din urmă efectuată. Întârzierea este deja irevocabilă şi va influenţa pe vecie scoringul debitorului. Asemenea datorii sunt vândute în mod obişnuit unor terţe companii financiare.

Comerţul cu informaţii transcende graniţele ţării, iar cele mai mari companii din branşă (Equifax, LexisNexis şi ChoicePoint) operează în întreaga lume. Ele sunt cunoscute ca brokeri de informaţii comerciale şi reprezintă afaceri uriaşe, care utilizează tehnici avansate, având milioane de abonaţi şi miliarde de nume înscrise în bazele lor de date. De asemenea, aceste companii achiziţionează informaţii din bazele de date ale altor ţări. Caracterul informaţiilor personale deţinute de ele nu se rezumă la relevanţa în cazul acordării unui credit şi nici la furnizarea de referinţe angajatorilor. Informaţiile lor nu sunt vândute doar în domeniul industriei şi comerţului, ci şi agenţiilor guvernamentale şi poliţiei.

LexisNexis a admis recent posibilitatea ca datele personale ale 310 000 de cetăţeni americani să fi fost furate în timpul unei căderi a sistemului de securitate, la începutul lui 2005. Când au fost pentru întâia oară interpelaţi pe marginea acestui incident, reprezentanţii companiei au declarat că disfuncţiile

sistemului de securitate au afectat doar câteva dintre numeroasele lor baze de date, conținând detalii a doar 32 000 de persoane – cam 10% din numărul real. LexisNexis a adăugat că penetrarea ilegală a bazelor de date, prin intermediul parolelor furate, a avut loc de cel puțin 59 de ori, ceea ce a mijlocit accesul hackerilor la adrese, la numere de Protecția Socială, precum și la alte date importante. Aceasta este numai ultima dintr-o lungă și de succes serie de încercări de a fura informații personale de identificare, care a afectat sute de mii de cetățeni din America de Nord și Europa.

În cursul depozițiilor în fața Congresului, grupuri de militanți pentru protejarea intimității și a drepturilor cetățenești, precum EPIC (Centrul pentru Intimitatea Datelor Electronice), au solicitat înăsprirea legislației privind brokerajul de date, utilizând drept argumente lipsa transparenței și a unei evidențe clare. Plângerile împotriva Experian și a altor agenții de scoring au fost nu puține și de toate felurile. Intimitatea a devenit o chestiune sensibilă într-o lume în care tot ceea ce facem este înregistrat și trecut într-o bază de date, iar normarea strictă a industriei de informații reprezintă o inițiativă care întârzie de ani buni. ConsumerInfo.com, subsidiară-furnizor de informații pentru companii precum Experian, Equifax și TransUnion, a fost acuzată de a fi încălcat legile Statelor Unite atunci când a făcut reclamă calculării „gratuite“ a scoringului propriu, care, odată făcută comanda, angaja clientul într-o relație de tip abonament, pe termen lung și cu costuri ridicate, fără a-l înștiința în privința condițiilor contractului (inclusiv a posibilităților de reziliere). Compania a fost acuzată, de asemenea, că și-a sporit veniturile prin suscitarea de temeri în legătură cu acuratețea scoringurilor, și provocând un val de cereri de vizualizare a rapoartelor prin intermediul propriului site.

Procesul împotriva ConsumerInfo.com a fost intentat de EPIC, care a atras atenția asupra absurdității situației în care o

agenţie de scoring face reclamă unei subsidiare, prin care clientul plăteşte pentru a verifica societatea-mamă, precum şi alte firme cărora aceasta le-a vândut informaţii. EPIC a folosit oportunitatea ca pe o modalitate de a solicita o legislaţie strictă a tuturor agenţiilor de scoring, forţându-le să ofere posibilitatea de a-şi vizualiza gratuit propriul raport. Pentru acest serviciu, în Marea Britanie se percepe o taxă de trei lire sterline. Mesajul publicitar al ConsumerInfo.com evidenţia faptul că undeva, în industria marketingului de date, se prea poate să existe o companie care vehiculează informaţii greşite despre tine. Problema rezidă în faptul că acea companie ar putea fi chiar cea care îşi face reclamă. Iată-l pe Kafka, în toată splendoarea sa.

Însă se poate şi mai rău. Când consumatorii sunt de acord să colaboreze cu un serviciu de monitorizare a scoringului pe bază de abonament, li se cer informaţii personale pentru a le fi validată identitatea. Creditorul are dreptul de a transmite mai departe aceste informaţii tuturor abonaţilor firmelor afiliate la agenţie. Consecinţa este că majoritatea persoanelor care doresc să-şi protejeze intimitatea renunţă, fără să-şi dea seama, cu totul la ea. Asta înseamnă că utilizatorii care doresc să se aboneze la agenţiile de scoring, pentru a avea cât de cât control asupra informaţiilor ce îi privesc şi pentru a-şi proteja propria intimitate şi corectitudinea datelor, obţin în realitate tocmai contrariul. Practicile de marketing ale agenţiilor de scoring, bazate pe exploatarea temerilor consumatorilor privind caracterul posibil eronat al rapoartelor, sunt, fără dubiu, îndoielnice din punct de vedere moral.

Simon Davies, directorul sucursalei britanice a Privacy International, este specialist în dezvoltarea companiilor care vehiculează informaţii personale şi are o experienţă îndelungată în problemele ce apar în acest domeniu. Privacy International şi grupul asociat EPIC au fost implicate în mai multe confruntări

cu firme precum ChoicePoint, a căror creștere, mai ales după 11 septembrie 2001, a fost spectaculoasă.

ChoicePoint, cu sediul în Georgia, Statele Unite, vinde informații către – printre alții – asigurători, agenții guvernamentale și industria marketingului. Conform raportului său trimestrial, înaintat Comisiei pentru Securitate și Schimb, ChoicePoint vinde „solicitări de despăgubiri, rapoarte privind autoturismele deținute, arhive ale poliției, informații privind creditele și calculul probabilităților îndeplinirii angajamentelor financiare ulterioare, (...) experiențe profesionale și rezultate ale controalelor antidoping, rezultate ale căutărilor în arhivele publice, date de stare civilă, servicii de verificare a veridicității titlurilor și calităților oficiale deținute, rapoarte de audit legal și contabil, date din Registrul Comerțului, servicii de identificare după ADN, servicii de autentificare și de localizare a persoanelor și acționarilor, (...) listare, servicii de call center și de administrare a bazelor de date și a unei campanii (...)".

De când s-a desprins de Equifax, în 1997, compania a acumulat un procent semnificativ din piața brokerajului de informații comerciale, prin preluarea a 38 de alte firme similare, fiind în prezent unul dintre cei mai importanți jucători din domeniu. Aceste achiziții includ nume precum Pinkertons inc, National Data Retriever inc, CITI Network, Bode Technology și Accident Report Services, printre multe altele. Conform *Wall Street Journal*, ChoicePoint a furnizat recent informații personale unui număr de cel puțin 35 de agenții guvernamentale, compania având în același timp în derulare contracte cu grupuri de impunere a legii în valoare de mai multe milioane de dolari.

Printre informațiile tranzacționate de ChoicePoint se numără și cele de identificare cu care începe un raport de scoring. Adică numele și adresa persoanei, numele soției, adresa anterioară, numărul de telefon, numărul de la Protecția Socială și angajatorul curent. Compania mai pune la dispoziția abonaților

serviciul numit „etalon preangajare", care cuprinde rapoarte financiare, verificare de diplome şi scrisori de recomandare, cazier (dacă există), încălcări ale Codului Rutier, verificare a datelor de la Protecţia Socială. O altă facilitate e dată de aşa-numita „estimare a bunurilor", care se referă la averea pe care o deţine o persoană. ChoicePoint mai oferă posibilitatea contractării căutărilor cu probabilitate redusă, ceea ce, în doar câteva minute, înlesneşte agenţiilor de păstrare a ordinii publice accesul la profilul complet al unei persoane, având drept punct de pornire un simplu prenume sau o adresă parţială. Aplicaţia în cauză se numeşte SmartSearch. Introducând în baza de date toate detaliile cunoscute despre o persoană, cum ar fi numele, vârsta, oraşul sau regiunea de reşedinţă probabile, programul poate indica unica persoană care întruneşte toate aceste criterii, afişând totodată adresa actuală a acesteia. Însă ChoicePoint nu deţine doar o listă a adreselor rezidenţiale, ci şi una cu personalul militar american şi britanic ori cu deţinătorii de aparate de zbor şi de ambarcaţiuni, pentru a facilita localizarea unei persoane.

Unul dintre produsele cele mai populare ale ChoicePoint este aplicaţia complexă AutoTrackXP, care permite ataşarea unei cantităţi semnificativ mai mari de informaţie la fişa unei persoane, prin intermediul aşa-numitelor „servicii de asociere". Acestea descoperă numeroase conexiuni între subiect şi alte date personale obţinute la nivel naţional, provenind, de pildă, de la clienţi şi birourile de taxe şi impozite. AutoTrackXP poate, de exemplu, să creeze legături între adresele anterioare ale unei persoane şi numele tuturor celor care au indicat aceeaşi adresă în documente precum carnetul de conducere.

Detaliile adiţionale includ permisele de tot felul aflate în posesia unui subiect, cum ar fi cele de conducere, de pilotaj sau de deţinere a unei arme de foc. De asemenea, elemente incluse în cartea de muncă, informaţii privind afacerile persoanei, scrisori de recomandare, calificări şi adeziuni, bunuri deţinute, bunuri

tranzacţionate sau cedate, actele aferente deţinerii sau conducerii unui vehicul, a unei bărci sau a unui aparat de zbor, numărul de Protecţie Socială, precum şi orice informaţii din arhive publice, cum ar fi arestări, acuzaţii, sentinţe legale ori falimente. Acest produs mai furnizează liste telefonice complete şi servicii de individualizare a unui abonat după numărul de telefon utilizat.

ChoicePoint a dezvoltat o tehnică numită „căutarea Soundex", bazată mai degrabă pe modul în care un nume este rostit decât pe felul în care este el scris. Mai mult, informaţiile oferite îi pot viza pe vecini sau pe membrii familiei unui suspect. De fapt, Soundex va construi un profil complet, conţinând informaţii contextuale privind mediul social căruia îi aparţine subiectul, cum îşi petrece el timpul liber, cum ajunge la serviciu, de unde îşi face cumpărăturile zilnice şi unde merge cu maşina.

Că o organizaţie de asemenea dimensiuni, care are drept obiect de activitate obţinerea şi diseminarea unei cantităţi uriaşe de informaţii personale, ar trebui să fie normată la sânge, este o ipoteză de bun-simţ. Şi totuşi, multe dintre produsele oferite nu se supun legislaţiei americane în vigoare. Unele produse de „dosar personal", precum raportul AutoTrackXP al ChoicePoint, sunt vândute fără ca respectarea US Fair Credit Reporting Act, lege americană care reglementează în linii generale, colectarea, distribuirea şi utilizatrea informaţiilor cu privire la creditele de consum, să fie obligatorie.

Comisia Federală pentru Comerţ (FTC – Federal Trade Commission) investighează în prezent activitatea ChoicePoint şi a altor brokeri de informaţii. Ancheta a fost lansată, în parte, ca urmare a unei plângeri înaintate de organizaţiile de respectare a drepturilor cetăţeneşti, în decembrie 2004. Aceste organizaţii au solicitat o investigaţie a „produselor tip dosar personal" oferite de brokerii de informaţii, printre care ChoicePoint. Cei de la EPIC sunt de părere că asemenea servicii constituie „rapoarte de consumator" şi se supun prevederilor Fair Credit Reporting Act.

Astfel stând lucrurile, atât furnizorul, cât şi clientul său se supun, la rândul lor, prevederilor actului menţionat. O chestiune intens dezbătută a fost dacă firmele ori agenţiile de detectivi particulari sau forţele poliţieneşti sunt îndreptăţite să aibă acces la datele vehiculate fără ştiinţa ori permisiunea persoanei la care se referă. EPIC – şi nu numai – consideră că transmiterea către poliţie a datelor personale furnizate de către o persoană în scopul primirii unui credit, fără ştirea acesteia, reprezintă un abuz. Cei mai mulţi consumatori sunt, fără îndoială, împotriva ideii de transmitere a informaţiilor personale pentru a servi unui scop diferit de cel pentru care ele au fost raportate iniţial. Deşi, în Marea Britanie, Legea protecţiei informaţiilor este menită să rezolve această dilemă, rareori s-a ajuns ca ea să fie invocată în sălile de judecată.

Rapoartele AutoTrackXP sunt similare ca scop şi utilizare scoringurilor standard, protejate de către lege. EPIC susţine că, prin vânzarea datelor personale fără respectarea prevederilor actului menţionat, ChoicePoint eludează scopul pentru care a fost instituită această lege federală privind restricţionarea informaţiilor cu caracter privat. Conform EPIC, companiile precum ChoicePoint şi produsele ca AutoTrackXP ţin de o epocă apusă, aceea în care legislaţia de protejare a subiecţilor companiilor de recoltare a datelor încă nu fusese implementată. În trecut, asemenea firme nu trebuiau să dea socoteală nimănui şi vehiculau adesea informaţii inexacte, falsificate ori irelevante despre persoane fizice. Uneori, într-o industrie de amploarea celei a colectării informaţiilor, profilurile puteau fi falsificate deliberat, pentru a creşte în mod artificial preţul asigurărilor sau al creditelor. Efectul era trecerea subiecţilor, în mod nejustificat, pe o listă neagră a persoanelor cu grad ridicat de risc, astfel încât ei erau puşi în situaţia de a plăti mai mult furnizorului de credit sau de asigurare (în general companii mai puţin respectabile). După cum era de aşteptat, ChoicePoint a respins aceste acuzaţii şi a suscitat o dezbatere naţională pe marginea acestui subiect.

Şi alte probleme puse în discuţie de către militanţii americani pentru dreptul la intimitate sunt semnificative în chestiunea creşterii anvergurii brokerilor de date personale. O asemenea problemă o ridică un articol publicat în *Washington Post,* în care compania ChoicePoint este acuzată că se comportă precum un serviciu secret, concluzia fiind că este necesar ca industria obţinerii informaţiilor să se supună unei noi legislaţii, dat fiind modul de utilizare a datelor personale. Articolul face referire la uriaşul capital de încredere câştigat de brokeri în privinţa informaţiilor ce pot fi folosite în investigaţii oficiale. După 9/11, ponderea utilizării datelor personale a crescut exponenţial în Statele Unite şi Marea Britanie. Este, de bună seamă, de importanţă vitală ca informaţiile folosite în scopul creării giganticelor baze de date antiterorism, precum CAPPSII, să fie reale şi ca practicile neguţătorilor de date să fie perfect transparente. ChoicePoint se bucură de aproximativ 100 000 de clienţi, printre care 7 000 de agenţii de impunere a legii. Cifrele nu includ clienţii din Marea Britanie ori Europa.

Dovezile înaintate Comisiei Federale pentru Comerţ de către EPIC includ o copie a listei de mailing a Politechbot.com. Un detectiv particular, utilizator al ChoicePoint, susţine că firma incriminată arhivează rapoartele de audit ale clienţilor care au avut acces la informaţii cu caracter personal. Dovada furnizată de EPIC este utilă, deoarece instanţele de păstrare a ordinii publice nu pot fi auditate şi nu a existat niciodată o situaţie în care un broker de informaţii să dea un utilizator pe mâna justiţiei, ca urmare a dovezilor furnizate de un astfel de audit, conform căruia acel utilizator a abuzat de serviciile furnizate.

EPIC a înaintat, de asemenea, copia unui documentar de televiziune intitulat *Cineva te urmărește,* difuzat pe 18 decembrie 2004 de Discovery Times Channel şi care s-a bucurat de o largă audienţă în Statele Unite. În film, doi investigatori particulari demonstrează cât de simplu poate fi ca, prin intermediul

unei agenţii de date, să obţii accesul la numărul de Protecţie Socială al unui străin, la date privind traiectul profesional al acestuia ori la alte informaţii, şi asta fără ca nici un fel de justificare legală să fie necesară.

Apoi, în februarie 2005, industria protecţiei informaţiilor a fost zguduită de una din cele mai uimitoare declaraţii făcute vreodată. Compania ChoicePoint a fost obligată să anunţe că a vândut informaţiile personale a cel puţin 145 000 de cetăţeni americani, majoritatea din California, unei reţele infracţionale specializate în furtul de identitate. Poliţia din California a raportat, între timp, utilizarea de către infractorii-clienţi ai ChoicePoint a materialului achiziţionat în schimbarea neautorizată a adreselor a cel puţin 750 de persoane, iar anchetatorii sunt de părere că au fost compromise informaţii personale a până la 400 000 de persoane din întreaga ţară. Organizaţiile de militanţi pentru respectarea drepturilor cetăţeneşti au fost scandalizate şi au cerut companiei să îi înştiinţeze pe cei ale căror informaţii au fost transmise membrilor reţelei în ceea ce priveşte natura şi conţinutul datelor în cauză. Nu doar din raţiuni de corectitudine şi dreptate, susţin aceştia, ci şi pentru a răspunde temerilor generale privind siguranţa publică.

Apoi, în martie 2005, în cadrul unei audieri în faţa Comitetului Senatorial pentru Bănci din California, companiile de administrare a informaţiilor, cum sunt ChoicePoint, LexisNexis şi Acxiom, au fost aspru criticate de senatoarea Jackie Speier, preşedinta comitetului. Ea a dorit să afle cum au putut sistemele ChoicePoint să fie înşelate cu atâta uşurinţă de către un grup de infractori cu un nivel rudimentar de pregătire, precum şi din ce motiv compania nu a raportat scurgerea de informaţii de îndată ce aceasta a fost descoperită. În replică, ChoicePoint şi-a cerut scuze pentru faptul de a fi vândut informaţii unor infractori şi a afirmat că va „sista vânzarea de produse informaţionale conţinând date personale sensibile“, incluzând aici numerele de

Protecţie Socială şi de înmatriculare a autovehiculelor, „cu excepţia cazurilor când este vorba de un beneficiu sau o tranzacţie orientate către consumator“ sau când produsele „sunt utilizate în interesul structurilor federale, statale sau locale ori cazuri penale“.

Multora, acesta li se va fi părut un răspuns prea prudent, având în vedere consecinţele scurgerii de informaţii. Compania a declarat că firmele mici vor putea în continuare achiziţiona rapoarte personale, însă se pare că numerele de Protecţie Socială nu vor mai figura în ofertă. De asemenea, ChoicePoint a anunţat că lucrează la un sistem care să ofere acces la produsele sale informaţionale. Însă persoanele particulare nu vor putea să îşi corecteze înregistrările provenind din arhivele publice, nici măcar în situaţiile în care acestea au fost redactate eronat. Cu toate acestea, numărul de Protecţie Socială va fi eliminat automat din aceste înregistrări.

În timpul audierii din California, directorul comitetului a cerut brokerilor de informaţii clarificări în privinţa propriilor definiţii a ceea ce reprezintă date „sensibile“, precum şi dacă termenul include numerele de Protecţie Socială sau de înmatriculare a autovehiculelor. Când acestea apar în arhivele publice, LexisNexis, de pildă, nu le consideră ca fiind sensibile şi le vinde fără cea mai mică ezitare. Senatorul Speier a declarat că este de părere că, în ochii multor oameni, aceste detalii sunt „cu adevărat cât se poate de sensibile“, adăugând că „noţiunea de «sensibil» a brokerilor de informaţii nu pare să reflecte realitatea“.

ChoicePoint a folosit în reclamele sale frica drept mijloc de a-şi promova serviciile, susţinând, de exemplu, că previne agresiunile pedofililor asupra copiilor şi că bazele sale de date au ajutat la găsirea multor copii dispăruţi. Senatorul Speier i-a întrebat pe cei de la ChoicePoint cât din procentul activităţii lor reprezintă localizarea acestor copii dispăruţi, întrebare rămasă fără răspuns.

EPIC nu numai că a condamnat direct reformele propuse de ChoicePoint, considerându-le „inadecvate“, dar a şi subliniat faptul că ele nu rezolvă protejarea datelor private în brokerajul de informaţii comerciale. Mai cu seamă, aceste schimbări nu obligă şi firmele rivale, astfel încât alţi brokeri de date pot continua nestingheriţi să vândă detalii precum numărul de Protecţie Socială oricui găsesc de cuviinţă.

EPIC a adăugat că „nici măruntele schimbări de procedură [propuse de ChoicePoint], nici revelarea faptului că au existat o serie de scurgeri de informaţii la mai multe bănci şi universităţi importante nu au adus atingeri majore unei pieţe dubioase complexe, a vânzării şi revânzării de informaţii personale, în continuare vulnerabile în faţa unor fraude similare“.

Se pare că ChoicePoint are de gând să tranzacţioneze în continuare rapoartele din arhive publice, aflate în afara reglementărilor, către firmele mici, de data aceasta cu numerele de Protecţie Socială şi de înmatriculare a autovehiculelor „trunchiate“, adică prescurtate. Însă marile companii şi forţele poliţieneşti vor putea obţine în continuare rapoarte complete, conţinând toate „informaţiile sensibile“ posibile. Încă nu se ştie cu precizie cum va fi „trunchiat“ numărul de Protecţie Socială. Există voci care susţin că va fi posibil ca firmele mici – şi nu numai ele – să folosească sistemul în sens invers, obţinând astfel numărul întreg. O soluţie ideală ar fi, fără îndoială, eliminarea cu totul a acestui număr din rapoarte, mai degrabă decât „trunchierea“ sa, la care există riscul de a putea fi depistat numărul original prin compilarea diferitelor surse.

Conform unui raport al Forumului Mondial pentru Intimitate, rapoartele de informaţii publice ale ChoicePoint au o „rată ridicată de eroare“. În etalonul propus, 90% din rapoartele obţinute conţineau greşeli, multe din acestea grave, iar altele de-a dreptul ridicole, cum ar fi indicarea altui sex în dreptul unor persoane. Constatările iniţiale ale analistului Forumului,

Pam Dixon, sunt susţinute şi de relatările alarmante ale altor persoane care şi-au citit propriile rapoarte ChoicePoint, din care au fost excluse informaţiile reglementate. După parcurgerea propriului dosar, cercetătorul Richard Smith a declarat că acesta „conţinea mai multe neadevăruri decât informaţii corecte". Elizabeth Rosen, infirmieră cu domiciliul în California şi una din multele victime ale scurgerii de informaţii ChoicePoint, a descoperit că din şase pagini, câte avea dosarul său, cinci conţineau erori. De pildă, raportul o indica în mod greşit drept funcţionară în Texas, având o căsuţă poştală privată la *Mailboxes Etc.* şi deţinând, printre mai multe afaceri, un magazin de delicatese numit Zach's. Doamna Rosen a amintit, în cadrul anchetei, despre frustrarea ei atunci când compania a refuzat, iniţial, să-i prezinte dosarul complet şi despre multele demersuri care s-au dovedit a fi necesare pentru a obţine datele în cauză. Întrebat de ce compania sa a refuzat să înmâneze un raport solicitat persoanei la care se referea, reprezentantul ChoicePoint nu a putut oferi un răspuns.

ChoicePoint afirmă acum că în viitor oamenii vor putea avea acces la rapoartele conţinând informaţii publice care nu se supun legilor în vigoare, dar nu vor avea dreptul de a corecta acele informaţii. Motivul invocat de ChoicePoint este acela că informaţiile nu pot fi corectate, dat fiind că ele provin din arhive publice. Însă s-a dovedit deja, în repetate rânduri, că ChoicePoint a încurcat informaţii referitoare la indivizi diferiţi. Astfel, Deborah Pierce, care a reuşit să-şi obţină „dosarul naţional complet" de la ChoicePoint, a descoperit cu stupoare din el că ar putea avea cazier în Texas. Că o persoană din baza de date a ChoicePoint are cazier în Texas se prea poate să fie adevărat, dar acea persoană nu este cu siguranţă Deborah Pierce.

Potrivit lui Simon Davies de la Privacy International din Londra, nimic nu poate obliga ChoicePoint să îşi respecte promisiunile de a-şi şi menţine practicile nou-implementate. În

ultimii ani, s-a dovedit că mai multe companii mari, printre care eBay.com,Amazon.com, drkoop.com şi yahoo.com, au modificat setările de siguranţă ale utilizatorilor sau au schimbat propriile politici de limitare a accesului la informaţii personale în detrimentul utilizatorilor. Din punct de vedere legal, ChoicePoint se află într-o poziţie favorabilă încălcării propriilor angajamente, dat fiind că nu recunoaşte existenţa unei legături directe cu consumatorii, care ar putea servi drept pretext pentru o acţiune în instanţă. Pentru ChoicePoint, „consumatorii“ sunt companiile care achiziţionează informaţii, nu persoanele la care se referă acele informaţii. Protecţie Socială

ChoicePoint a emis un comunicat de presă în care a anunţat că îşi rezervă dreptul de a tranzacţiona informaţii personale „sensibile“ către persoane juridice pe mai multe căi. Astfel, datele sensibile vor fi vândute „pentru a asista la efectuarea tranzacţiilor orientate către client, atunci când sunt necesare unele informaţii pentru a consfinţi sau menţine o relaţie de afaceri, (...) pentru a oferi instrumente de autentificare şi prevenire a infracţiunilor vizând mari corporaţii, cu care consumatorii au deja relaţii, (...) pentru a ajuta guvernele federale şi statale, administraţiile locale, poliţiile şi agenţiile de informaţii în îndeplinirea misiunilor lor importante“. Ce reprezintă oare exact „tranzacţii orientate către client“? Şi când este nevoie de informaţii „pentru a consfinţi sau menţine o relaţie de afaceri“? Această declaraţie nu este altceva decât o bâlbâială a unui PR-ist năucit, care se trezeşte din senin că trebuie să înfrunte focul încrucişat al întrebărilor reprezentanţilor massmediei.

ChoicePoint se află în poziţia fericită de a putea decide pe cont propriu ce anume reprezintă „beneficiul consumatorului“. În trecut, compania a avut o încercare de a furniza propria definiţie a acestui termen, susţinând că se va împotrivi demersurilor de a şterge orice fel de informaţie din bazele de date deţinute, deoarece „considerăm că ştergerea informaţiilor ar

reduce utilitatea acestor produse pentru afaceri, ceea ce ar fi, în cele din urmă, tot în detrimentul consumatorilor. Ce crede ChoicePoint că e bine pentru consumatori nu e însă și ceea ce consumatorii cred că e bine pentru ei înșiși.

Politica ChoicePoint îi permite companiei să vândă dosare complete, în scopul prevenirii fraudelor. Inițiativă teoretic lăudabilă și de bun-simț, însă, practic, aproape orice tranzacție reprezintă o potențială fraudă. Dacă se optează pentru păstrarea acestei politici, ea îi va permite companiei să continue să vândă informații personale, chiar și atunci când riscul de fraudare este minim ori este utilizat drept pretext pentru colectarea în alt scop a informațiilor.

În cursul audierilor din California, ChoicePoint a ridicat un pic cortina, dezvăluind structura principalului său obiect de activitate: un procent de 5% din afacere e reprezentat de „distribuția informațiilor către polițiile locale și federale, pentru a înlesni investigațiile în curs“, iar 6% – de „ajutorul acordat cabinetelor de avocatură, instituțiilor financiare și altor organizații, în scopul reducerii riscurilor prin informații și autentificare de date, inclusiv suport juridic ori de date necesare recuperării datoriilor“. Un alt procent de 20% îl reprezintă vânzarea de software și tehnologie fără legătură cu distribuirea de informații personale.

În dezbaterile legate de propriile strategii, ChoicePoint nu specifică întotdeauna dacă se referă la rapoartele reglementate sau nereglementate legal, producând confuzie atât în rândul publicului, cât și printre legiuitori. Aproximativ 60% din afacere îl reprezintă „tranzacțiile inițiate de către consumator“, cele mai multe reglementate de Fair Credit Reporting Act, legea ce reglementează utilizarea informațiilor necesare pentru credite. Astfel de tranzacții includ eșantionarea preangajare și servicii de evaluare a preasigurării, estimarea riscurilor unui potențial chiriaș, oferirea de informații de maximă importanță utilizatorilor,

întocmirea de asigurări împotriva daunelor. Aproape 9% din afacere sunt serviciile de marketing, care nu implică distribuția de date personale, dar care se supun reglementărilor statale și federale ce interzic trimiterea nesolicitată, telefonic sau prin e-mail, a informațiilor către public.

Faptul că propunerile de „reformă" ale ChoicePoint nu limitează vânzarea de informații personale către poliții – fie ele federale, locale sau statale –, către poliția britanică sau către departamentele de finanțe sau de imigrare, ar trebui să reprezinte un semnal de alarmă pentru oricine intră în vizorul companiei. Grupurile americane de militanți pentru drepturile cetățenești susțin că legiuitorii ar trebui să trateze problema traficului cu date personale nu ca pe o chestiune de securitate, ci ca pe un atentat la viața privată. Chiar și atunci când informațiile personale sunt utilizate securizat, rămâne problema tranzacționării lor către o paletă largă de organizații, persoanele implicate neavând nici un cuvânt de spus în această privință.

Cam acesta este viitorul pieței informaționale. Cererea de date personale crește în America, în Marea Britanie și în restul Europei. Piesele-lipsă sunt regulamentele și legislația aferente. Suntem permanent monitorizați, iar ceea ce este înregistrat se vinde. Când vom începe, în cele din urmă, să ne exprimăm temerile privind pierderea dreptului nostru la viață privată, s-ar putea să fie deja prea târziu.

CAPITOLUL IV

Intră, numărul 15788659/54377...

Cei mai mulţi dintre noi ne credem îndreptăţiţi să presupunem că toate datele şi informaţiile pe care statul le deţine despre noi sunt protejate şi că formularele pe care le completăm pentru Administraţia Financiară sau pentru Biroul de Pensii rămân între noi şi inspectorul nostru fiscal. Fişele cu starea sănătăţii noastre, am crezut întotdeauna, fiind atât de laborios puse pe hârtie de către medicul de familie, vor rămâne disponibile doar autorităţilor interesate şi nu vor ajunge nicicum mai departe. Suntem încredinţaţi că acelaşi lucru se va întâmpla şi cu rapoartele păstrate de instituţii precum Vamă şi Accize. Evident, credem acelaşi lucru despre informaţiile privindu-i pe copiii noştri, deţinute de autorităţile educaţionale locale, despre baza de date ADN sau de recunoaşterea facială a poliţiei, Biroului de Informaţii privind Infractorii şi multor alte arhive de date. Autoritatea pentru Şoferi şi Autovehicule (DVLA) este în posesia unor cantităţi masive de informaţii despre noi şi despre maşinile pe care le conducem, şi ea publică analize nesfârşite şi rapoarte savante privind obiceiurile noastre la volan. De fapt, majoritatea contactelor noastre cu statul sunt înregistrate şi transcrise, informaţiile putând fi folosite ulterior ca dovezi împotriva noastră.

În fiecare zi din viaţă, intrăm în relaţie cu statul. Împrăştiem informaţii despre noi diferitelor agenţii naţionale. Fiecare

vizită pe care o facem la medic este înregistrată în baza de date a Serviciului Naţional de Sănătate (NHS), în care evoluţia sănătăţii noastre devine un grafic ce ne acoperă întreaga viaţă şi este accesibil secretarului de stat şi, de acolo, oricui consideră acesta că trebuie să-i fie accesibil. Schimbările de domiciliu sunt înregistrate de către Administraţia Financiară, DVLA şi Departamentul Protecţiei Sociale, iar bunăstarea noastră este cunoscută de către bănci, companiile de scoring şi agenţiile de pensii. Baza de date naţională computerizată a poliţiei şi cea a Serviciului de Procuratură al Coroanei, deţin un raport complet, chiar dacă nu întru totul corect, al istoriei noastre infracţionale. Baza naţională de date ADN are înregistraţi în prezent două milioane de cetăţeni britanici, iar numărul lor creşte rapid. Telecom şi companiile de telefonie mobilă deţin numeroase cunoştinţe despre orice persoană adultă din Marea Britanie. De fiecare dată când utilizezi un telefon mobil, locaţia ta exactă este detectată, la fel ca şi destinaţia apelului. Serviciile de utilitate publică au şi ele cantităţi enorme de informaţii privind obiceiurile noastre cotidiene. Acum, când apa este contorizată în multe zone din Marea Britanie, companiile din domeniu îţi pot spune chiar şi dacă mergi regulat la toaletă în timpul vreunei emisiuni de televiziune populare.

Administraţia Financiară încă se luptă cu dificultăţile întocmirii unei baze de date imense, în care fiecare contribuabil din ţară va fi înregistrat şi confirmat de o altă sursă. Conform estimărilor curente, această bază de date va costa 30 de miliarde de lire sterline atunci când va fi completă, deşi probleme de programare au tot pus piedici planului şi, probabil, costul final va fi considerabil mai mare. Recenta fuziune dintre Administraţia Financiară şi Departamentul Vamă şi Accize a creat potenţial o unitate mult mai puternică de strângere a impozitelor, care va putea oferi o perspectivă cuprinzătoare asupra declaraţiilor noastre de venit şi să elimine anomaliile. Totuşi, cum se întâmplă

cu cele mai multe baze de date, eficienţa sa va depinde de acurateţea datelor introduse şi de abilitatea personalului de a o folosi. Chiar dacă informaţiile sunt înregistrate detaliat, Administraţia Financiară va fi mereu obligată să se bazeze pe formulare sau plicuri maro cu salarii şi nu se poate aştepta ca toate impozitele declarate să fie precise. Ea nu doar strânge taxe, ci îi forţează pe angajatori, în mod curent, să deducă rambursarea împrumuturilor studenţeşti din salariile angajaţilor lor, obligând astfel întreprinderile să devină colectori atât de debite, cât şi de impozite, în numele guvernului. Biroul de Pensii, care face şi el parte acum din Administraţia Financiară, are o bază de date specială, în care se regăsesc contribuţiile noastre la asigurările de stat, înregistrările locurilor de muncă şi situaţia noastră financiară încă de la 16 ani. Cantitatea de informaţii oferite Administraţiei Financiare şi înregistrate fără voia noastră poate fi confruntată şi cu detaliile privind conturile noastre bancare şi de economii şi va fi pusă la dispoziţia agenţiilor de investigaţii precum Biroul pentru Combaterea Fraudelor Grave sau departamentul de colectare a taxelor al Administraţiei Financiare, aflat în Worthing. Desigur, aceste agenţii nu se bazează numai pe datele aflate în acest mod, ci angajează şi funcţionari ale căror sarcini constau în investigarea contribuabililor şi „pescuirea“, din istoria lor de salariaţi, a unor venituri frauduloase sau neconforme cu realitatea.

În 2004, Serviciul Naţional de Sănătate (NHS) a anunţat lansarea programului său de dezvoltare a unei baze de date computerizate. Contractele destinate acestui proiect, condus de departamentul IT al NHS, valorau iniţial 6,2 miliarde de lire sterline. Cum era de aşteptat, proiectul a depăşit curând bugetul, costurile sale fiind estimate în 2005 la 31 de miliarde de lire. Acest program implică transferul unor ani întregi de fişe scrise de mână din înregistrările medicilor generalişti într-un computer naţional, aflat în Manchester. Transferul informaţiilor va fi realizat cu precădere de experţi IT externi. Conform declaraţiilor

lui John Hutton, ministrul Sănătăţii, guvernul oferea cetăţenilor posibilitatea de a alege nivelul de securitate de care să se bucure dosarul lor. „Pacienţii vor fi întrebaţi dacă doresc ca înregistrările lor medicale să fie incluse în baza de date sau dacă preferă ca aceste informaţii să fie scoase din sistem şi protejate într-un «plic sigilat» electronic, care va restricţiona accesul, exceptând cazurile de extremă urgenţă." Ulterior, managementul acestui proiect a modificat această garanţie aparent liniştitoare, evidenţiind faptul că pacienţii care vor restricţiona astfel accesul la propriile dosare îşi vor asuma riscul ca personalul clinic să mai şi greşească în situaţii de urgenţă. Împiedicarea accesului la înregistrări va fi sinonimă cu o cantitate mai mică de informaţii disponibile imediat despre probleme medicale cunoscute, inclusiv reacţii alergice.

Baza de date a NHS va reprezenta una dintre cele mai complexe încercări de exploatare a datelor de până acum. Protecţia sa este de importanţă vitală pentru orice persoană din Marea Britanie care pune preţ pe sfinţenia vieţii sale intime. Totuşi, stă în puterea politicienilor şi a funcţionarilor publici să se asigure că nici măcar o informaţie medicală nu va ajunge pe mâini nepotrivite. Vor exista tot felul de legi, precum şi ameninţarea cu pedepse severe pentru hackerii care vor fi prinşi înfruptându-se din aceste date. Guvernul a afirmat că această bază de date prezintă avantaje pentru noi toţi, deoarece, graţie ei, putem fi siguri că medicul care ne tratează are acces la cele mai recente şi mai corecte informaţii ce ne privesc. Baza de date va fi mai protejată decât sistemul tradiţional de hârţoage şi ea nu va face parte din informaţiile înregistrate pentru arhiva cărţilor de identitate. Oricum, profesioniştii din sfera sănătăţii au multe rezerve în privinţa acestui proiect. Înregistrările din domeniul sănătăţii publice ale britanicilor vor constitui o resursă nepreţuită pentru industria asigurărilor sau pentru agenţiile de menţinere a liniştii publice. Industriile medicamentelor

şi asigurărilor sunt multinaţionale şi prospere, iar valoarea înregistrărilor medicale ale unei întregi naţiuni li se va părea inestimabilă. „Dispozitivele de securitate“ nu înseamnă mare lucru, fiindcă medicina de urgenţă poate deveni un proces haotic, ce solicită profesionalism clinic şi tratament grabnic, aşa că accesul rapid la înregistrări va fi prioritar. Probabil vor exista multe ocazii, în cadrul unei secţii de urgenţă, în care securitatea bazei de date va coborî – şi e de înţeles – pe lista priorităţilor. Vechiul sistem de informaţii scrise era mult prea greoi pentru ca persoane neautorizate să-l poată accesa facil, după bunul plac şi în profunzime. Nici o astfel de dificultate nu îi va stânjeni însă pe hackerii care vor să intre în baza de date a NHS. Va fi imposibil să protejezi datele în cazul unui accident ce ar aglomera o secţie de urgenţă în care angajaţii împart un singur terminal de computer. Harold Cayton, de la Departamentul pentru Dezvoltarea Rapoartelor Medicale Naţionale, a afirmat că împărtăşirea informaţiilor privind pacienţii ar trebui să rămână o chestiune ce ţine de relaţia medic-pacient. Departamentul se pregăteşte să publice o „Garanţie a informaţiilor medicale“ (care, spune medicul meu, nu va valora nici cât hârtia pe care este tipărită!). Asociaţia Medicală Britanică (BMA) a solicitat guvernului asigurări şi dispozitive de siguranţă mai puternice. Unii medici generalişti şi câteva cabinete medicale chiar au refuzat să-şi predea înregistrările. Trebuie spus că pacienţii nu au dreptul de a decide asupra datelor pe care doctorii le stochează despre ei şi că nu există nici un medic generalist sau vreun alt corp profesional care să fie în mod clar răspunzător de protejarea informaţiilor strânse. Pare evident că multe dintre libertăţile cetăţeneşti vor fi puse în pericol.

Autoritatea pentru Şoferi şi Autovehicule (DVLA) face parte din Departamentul Transportului. Autoritatea funcţionează ca o bază de date computerizată încă din 1980, care ne emite permisele şi ne procesează taxele rutiere. Ea reprezintă

depozitarul înregistrărilor noastre auto şi istoria maşinilor pe care le-am avut de-a lungul vremii. DVLA notează, de asemenea, adresele posesorilor tuturor autovehiculelor, poliţele de asigurare, încălcările Codului Rutier şi pedepsele primite pentru acestea, interdicţiile de a conduce, permisele provizorii şi testele de conducere, precum şi fişele de întreţinere ale maşinilor noastre. Autoritatea caută mereu infracţiuni rutiere şi condamnări, clasificate după sexul şi vârsta celor ce le-au comis, precum şi obligă la noi testări de după condamnări pentru conducere periculoasă sau sub influenţa alcoolului. Analizează statistici cu privire la recidive, pierderi de drepturi şi supravieţuirea victimelor accidentelor. Examinează efectele pe care diverse medicamente şi droguri le au asupra şofatului şi consiliază sistemul judecătoresc în privinţa verdictelor. Astfel, DVLA este implicată în administraţia şi legislaţia privindu-i pe toţi şoferii din Marea Britanie. Arhiva sa este cuprinzătoare şi este folosită constant de forţele poliţieneşti din Marea Britanie şi din străinătate.

Baza de date conţine înregistrări ale maşinilor furate, informaţii ce sunt distribuite tuturor forţelor de poliţie, prin sisteme de identificare a numerelor de înmatriculare. De asemenea, arhiva este în mod curent pusă la dispoziţia companiilor de asigurări şi a Sistemului de taxare antiambuteiaj din Londra. Software-ul pentru sistemul DVLA a fost instalat de către Capita, subcontractorul IT al guvernului, care a externalizat în India dezvoltarea de programe de arhivare, pentru a exploata forţa de muncă ieftină din acest subcontinent asiatic. Organizaţiile de apărare a libertăţilor cetăţeneşti consideră că această mutare va face ca datele deţinute de DVLA să devină disponibile în acest stat în curs de dezvoltare. Autoritatea are o experienţă de decenii în prelucrarea datelor şi pretinde că „securitatea informaţiei este bine reglată". Însă nu destul de bine. Au existat numeroase exemple de informaţii accesate ilegal prin computerul cu arhiva permiselor de conducere al DVLA şi prin oficiul de verificări ale

cazierului[1] (CRB). Saul Dickinson, un apărător extremist al drepturilor animalelor, care a fost angajat al DVLA, a dat mai departe numele, adresele şi numerele de înmatriculare ale personalului unei ferme de cobai din Staffordshire. Aceste informaţii au fost folosite într-o campanie de terorizare a familiilor care lucrau la fermă. Dickinson a fost condamnat la cinci ani de închisoare.

Lipsite de resurse, forţele poliţieneşti din Marea Britanie primesc cu entuziasm revoluţia tehnologică. Testările pentru arhiva ADN a poliţiei au fost privatizate şi sunt luate mostre de la toate persoanele arestate sau implicate în orice fel în vreo infracţiune. În acest moment, există două milioane de indivizi incluşi în această bază de date, iar numărul lor va creşte rapid, ca urmare a modificărilor suferite de lege. Cei mai mulţi din arhivă nu vor fi niciodată condamnaţi pentru vreo infracţiune, dar, după regulile curente, informaţiile lor vor rămâne în baza de date cât vor trăi. Sunt luate mostre de salivă, fire de păr şi fluide corporale, iar apoi comparate cu mostrele găsite la locul infracţiunii. Riscurile informaţiilor ADN este că ele pot fi utilizate pentru a oferi date care n-au nici o legătură cu vreo infracţiune. De pildă, ele pot dezvălui amănunte ale unor relaţii de familie, inclusiv de paternitate, şi predispoziţii genetice pentru anumite boli, informaţii ce s-ar putea dovedi utile industriilor de medicamente şi de asigurări. Genewatch, un grup de apărare a libertăţilor cetăţeneşti îngrijorat de felul în care pot fi utilizate informaţiile oferite de genomul uman, consideră că ar trebui să existe un corp public independent, transparent şi responsabil, care să fie desemnat să ia decizii privind arhiva ADN. Mostrele ar trebui distruse după utilizare, spune Genewatch; trebuie interzise imediat cercetările genetice ce utilizează aceste

[1] Criminal Records Bureau a fost înfiinţat în 2002 în Marea Britanie pentru a verifica, înainte de angajare, cazierul potenţialilor angajaţi. (n.red.)

date; în plus, eficienţa acestei arhive în stoparea criminalităţii ar trebui analizată independent. Folosirea dovezilor ADN a dus deja la mari erori judiciare, în cazul unor femei acuzate că şi-au vătămat propriii copii. Cercetările genetice au fost deja desecretizate. Un proiect numit Biobanca Marii Britanii intenţionează să strângă şi să analizeze datele genetice ale unui număr de 500 000 de voluntari cu vârsta de cel mult 30 de ani. Obiectivul este de a identifica acele gene asociate unor maladii – informaţii de mare interes, fără dubiu, pentru domeniul asigurărilor de viaţă.

Computerul Naţional al Poliţiei (PNC) reprezintă o bază de date ce acoperă întreg teritoriul ţării şi include condamnările pentru delicte „înregistrabile“ – adică acelea pentru care vinovaţii pot fi trimişi la închisoare. Aceste înregistrări trebuie scoase din arhivă după zece ani sau după cinci ani, dacă persoana în cauză scapă pe cauţiune. De la trei condamnări în sus, înregistrarea rămâne în baza de date 20 de ani. Există, desigur, excepţii, cum sunt persoane condamnate pentru infracţiuni de natură sexuală, acte violente, molestarea copiilor şi persoanele fără discernământ care nu pot răspunde juridic pentru fapta lor. Arhiva PNC este disponibilă imediat unui număr de aproape un sfert de milion de poliţişti din Marea Britanie şi este extinsă permanent. Un nou sistem de recunoaştere facială este evaluat în oraşe din Yorkshire, Strathclyde, precum şi de câteva forţe de poliţie din regiunea Midlands. Recunoaşterea facială a fost utilizată frecvent în alte părţi, deocamdată fără succes. Ea presupune înregistrarea datelor biometrice faciale. Există 60 de părţi ale feţei identificabile separat, care formează împreună portretul unic al unui individ. Din nefericire, cam asta e tot. O fotografie pentru identificare a poliţiei, realizată şi arhivată digital după o arestare, este clară, iar subiectul ei – imobil. Faţa infractorului noaptea, în centrul plin de umbre al unui oraş, este cu totul altceva. În prezent, sistemul pare un experiment

costisitor și eșuat. Totuși, multe milioane de lire sterline din bugetul autorităților locale de poliție au fost deja cheltuite și vor trebui justificate cumva. Tehnologia recunoașterii faciale nu a fost încă testată în tribunalele britanice, dar cum putem fi siguri că acest lucru nu se va întâmpla în viitorul apropiat, ducând la identificări greșite și erori judiciare?

În întreaga țară, poliția colaborează cu autoritățile educaționale locale pentru a pune capăt chiulurilor. Pentru prima oară în Marea Britanie, copiii-problemă au fost înregistrați pe computere, în multe zone ale țării. Când sunt prinși, chiulangiii „recidiviști“ au mari șanse de a primi o „decizie de comportament antisocial“. În cazuri extreme, părinții lor pot fi – și unii chiar au fost – întemnițați. Stocarea datelor unor copii într-o arhivă națională reprezintă o problemă gravă. Organizațiile de apărare a libertăților cetățenești sunt îngrijorate că încă o barieră a fost dărâmată. Copiii sunt deja tratați ca infractori în Statele Unite, unde unei fetițe de cinci ani, care a avut un acces de furie în incinta școlii sale din Florida, i s-au pus cătușe și a fost luată din clasă de către ofițerii de poliție. Unii copii au mai fost închiși în Marea Britanie, dar includerea lor într-o bază de date a autorităților educaționale poate fi începutul unei periculoase spirale descendente. Deocamdată, nici chiar puștilor cu comportament deviant nu li se cere să poarte o carte de identitate când vin – dacă vin – la școală.

Cărțile naționale de identitate sunt utilizate în toată lumea. Ele variază ca funcții și ca integritate a datelor, precum ajutoarele de sănătate sau asistența socială. Unele sunt obligatorii, altele nu. Unele utilizează numere pentru a identifica purtătorul, dar cele mai multe au încorporată o bandă electronică. Cardul de plastic a înlocuit „hârtiile“ de identitate, fiindcă este mai greu de falsificat, iar producătorii de carduri știu să-și vândă marfa și pot cu ușurință să-și actualizeze în mod regulat sistemul, adăugând mai multe informații despre posesor și despre familia lui

sau ei, pe măsură ce acestea devin disponibile. Aproximativ 100 de ţări ale lumii au cărţi de identitate obligatorii. Totuşi, afirmaţia nu este valabilă pentru Statele Unite, Marea Britanie, Canada, Australia şi Noua Zeelandă. În Australia şi Noua Zeelandă, publicul a respins categoric, prin referendumuri, propunerea de introducere a unor cărţi de identitate pe timp de pace. Canada a abandonat iniţiativa unor cărţi de identitate biometrice în 2004. Şi, chiar şi după atacul din 9/11, propunerile zgomotoase de introducere a unei cărţi de identitate au fost respinse cu fermitate de Congresul Statelor Unite.

De obicei, cartea de identitate este introdusă într-o ţară din raţiuni ce ţin de rasă, politică, religie sau securitate. David Blunkett, fost ministru de Interne al Marii Britanii, a anunţat proiectul unei cărţi de identitate „pentru drepturi“ în octombrie 2001, imediat după tragedia de la turnurile gemene. Motivele sale erau de a înăspri măsurile antitero, îngreunându-le imigranţilor ilegali operaţiunile din Marea Britanie, şi de a contracara fraudarea ajutoarelor sociale. Cardul „pentru drepturi“ urma să devină o carte de identitate obligatorie, chiar dacă nu era numit aşa. Fiecare cetăţean care îl solicita ar fi trebuit să plătească 75 de lire sterline şi să ofere 50 de informaţii personale. Ideea a întâmpinat o opoziţie imediată. Fostul secretar de Interne Mike O'Brian a spus: „Miniştrii au admis deja că ţelul nostru este de a căuta să apărăm libertatea şi democraţia. Fiecare împrejurare în care suntem obligaţi să subminăm aceste valori va fi revendicată de terorişti ca o victorie“. S-a mai afirmat, pe bună dreptate, că existenţa cărţilor de identitate în Statele Unite nu ar fi putut împiedica atacul din 9/11.

Blunkett a bătut în retragere cu propunerea sa, însă a încercat introducerea cărţii de identitate din nou în februarie 2002. După un baraj de critici venite din Camera Lorzilor, el a înlăturat formula ambiguă „pentru drepturi“ şi a descris cardul exact cum era gândit să fie – o carte de identitate. Mai mult, a admis că nu

va fi obligatoriu să porți mereu acest card; totuși, el va fi cerut pentru a beneficia de ajutoarele de sănătate sau de asistența socială. Persoanele în căutarea unui serviciu vor trebui să prezinte cardul atunci când aplică pentru un loc de muncă sau alte „drepturi". Inițial, Partidul Conservator a susținut introducerea cardului, apoi s-a răzgândit și s-a opus. Cei care s-au împotrivit proiectului au fost acuzați că sunt prea „moi" în fața amenințării teroriste – o greșeală politică fatală. Proiectul de lege a fost retras înainte de anunțarea alegerilor generale din 2005, deoarece nu mai era suficient timp pentru ca el să treacă prin Parlament.

Dacă acest card va fi sau nu impus vreodată în Marea Britanie, asta depinde, pe de-o parte, de cursul evenimentelor și, pe de altă parte, de introducerea unor schimbări ale altor documente de identitate, cum ar fi pașapoartele cu amprenta posesorului. Un alt factor este publicul: oare cetățenii vor înțelege în totalitate cu ce se vor confrunta dacă se decid să aplice pentru cartea de identitate? Cei mai mulți oameni cred că este o banală bucată de plastic, dar de fapt e vorba de un sistem vast, complicat și cu bătaie lungă, care implică un nivel de utilizare fără precedent a informațiilor personale.

Unii politicieni susțin hotărât ideea unei cărți de identitate naționale, însă avantajele lor de pe urma sistemului nu sunt nicidecum clare. Ce se va întâmpla cu adevărat când și dacă va fi introdus acesta? Este un proiect de lege cu țintă limpede. Mai întâi, va fi un Registru Național de Identificare, care îi impune ministrului de Interne obligația de a crea un Registru Central al Populației, conținând informațiile personale ale tuturor cetățenilor britanici care au vârsta peste 16 ani. În al doilea rând, fiecărei persoane îi va fi alocat un număr unic, care va fi cunoscut ca Numărul Național de Înregistrare a Identității (NIRN). Acest număr va reprezenta elementul-cheie care va permite agențiilor guvernamentale să acceseze și să împărtășească informații despre noi toți. Articolul 5 spune că trebuie să răspundem eventualelor

cereri de a furniza date biometrice sau alte forme de identificare fizică, care pot fi o fotografie pentru recunoaştere facială sau imagini ale degetelor noastre arătătoare (utilizate în sistemul imigrării din SUA). Vom fi nevoiţi să achiziţionăm şi să purtăm un card de plastic, care permite confruntarea directă cu informaţiile din baza de date. Articolul 15 ne cere să prezentăm cardul ori de câte ori vrem să beneficiem de servicii publice. Iar articolul 6 afirmă că numărul „unic" şi registrul vor fi utilizate de tot felul de agenţii drept bază administrativă.

Va exista şi o „componentă de confruntare" privind înregistrările de date, conform căreia toate agenţiile guvernamentale au obligaţia de a se informa reciproc cu privire la modificările datelor noastre personale. Asta permite ca toate numerele noastre de înregistrare (precum cele de la serviciile naţionale de asigurare sau de sănătate) să fie strânse laolaltă. De exemplu, dacă informăm Departamentul Protecţiei Sociale că ne-am schimbat domiciliul, acesta este obligat să anunţe Serviciul Naţional de Sănătate, poliţia ş.a.m.d.

Articolul 19 al proiectului de lege permite divulgarea informaţiilor din registru, fără a fi nevoie de consimţământul nostru, către – printre multe alte agenţii – forţele poliţieneşti, serviciile secrete, Administraţia Financiară, Departamentul Vamă şi Accize, Forţele de Muncă, Biroul de Pensii şi Departamentul pentru Combaterea Crimei Organizate. Proiectul de lege va mai stabili o nouă gamă de infracţiuni şi contravenţii, creată pentru a se asigura că publicul îndeplineşte cerinţele cărţii de identitate.

Dacă privim astfel lucrurile, vom realiza că nu vom avea doar un card simpatic de plastic, aşa cum speram. Informaţiile de care guvernul pretinde că are nevoie sunt detaliate şi reprezintă o intruziune în viaţa noastră. Aspectul poate cel mai alarmant al proiectului este faptul că nu conţine nici o clauză conform căreia Parlamentul poate decide ce informaţii personale vor fi înregistrate în baza de date. Decizia este lăsată la latitudinea Ministerului

de Interne, care va putea să suplimenteze numărul informaţiilor solicitate după bunul său plac. Ministerul a declarat că va dori să ştie despre fiecare unde am locuit în trecut (inclusiv adresele complete şi codurile poştale) şi că ne va solicita „informaţii despre împrejurările în care datele înregistrate (inclusiv fotografii, amprente, înregistrarea irisului, numărul de asigurare sau al paşaportului, carnetul de conducere şi orice alt document oficial) au fost oferite altor persoane".

Se produc, totuşi, încălcări grave ale libertăţilor cetăţeneşti, prin furt de identitate, în Marea Britanie şi Statele Unite, cu toate că problema e mai puţin gravă în Europa. Germanii sunt încântaţi să poarte pretutindeni cărţi de identitate şi, la fel ca şi toţi membrii serviciilor armate din Marea Britanie, tolerează în general cerinţele cardului, fiindcă s-au obişnuit deja cu ideea. Însă sistemul german reprezintă o intruziune mult mai mică în viaţa privată decât cel propus pentru Marea Britanie. Americanii sunt obligaţi să-şi controleze viaţa şi să-şi conducă afacerile prin mijloace electronice. Lor li se cere mereu să dovedească faptul că sunt cine pretind că sunt. Practic, asta înseamnă că „elementele de date" personale sunt incluse în programele instalate pe mii de computere. Parolele, numerele de identificare fiscală, numele dinaintea căsătoriei, data naşterii, codurile poştale şi alte informaţii individualizatoare sunt folosite pentru autentificare. Problema e că aceste detalii pot fi uşor accesibile hackerilor şi, dată fiind răspândirea actuală a internetului wireless, dacă datele nu sunt criptate, ele pot fi accesate uşor de orice persoană din vecinătate care deţine echipamentul potrivit şi vrea să arunce un ochi în computerul tău. Fraudarea identităţii este marea problemă în Statele Unite. În 2002, FBI a arestat trei bărbaţi care furaseră 30 000 de rapoarte de scoring şi le vindeau, pentru a fi folosite în diverse combinaţii de însuşire abuzivă a identităţii. Hackerii au mai izbutit să se infiltreze într-o companie care procesează tranzacţii prin cartea de credit şi au

furat zece milioane de numere ale unor carduri AmEx, Visa şi Mastercard. Indiscutabil, vechile concepte confortabile de identitate privată nu se mai aplică în Statele Unite şi Marea Britanie.

Astfel de infracţiuni sunt tot mai numeroase, deoarece prea multe informaţii personale ale noastre sunt disponibile pentru infractorii hotărâţi. Aşa cum am văzut până acum, zi de zi, ceas de ceas, agenţiile de creditare, firmele de asigurări, băncile, supermarketurile şi operatorii de carduri inteligente colectează informaţii despre noi. Iar apoi le vând. Cei care supraveghează şi strâng date – în special companiile de evaluare a creditelor, precum Experian în Marea Britanie, sau neguţători de baze de date, precum Acxiom în Statele Unite – se opun reglementărilor guvernamentale şi pretind că acestea ne-ar face viaţa mai scumpă şi mai complicată. Creditele se obţin uşor. O companie americană numită Synovate, care urmăreşte solicitările de cărţi de credit pe e-mail, afirmă că anul trecut au fost trimise în SUA în jur de cinci miliarde de oferte electronice.

În întreaga lume se află în circulaţie în prezent peste trei miliarde de carduri Visa şi Mastercard, care generează profituri uriaşe pentru companiile emitente. În mod corespunzător, hoţii de informaţii au devenit din ce în ce mai pricepuţi în evitarea măsurilor de protecţie. În acelaşi timp, înregistrările agenţiilor de scoring au fost viciate de erori, deoarece majoritatea informaţiilor generate de operatorii de carduri au ca surse computere, nu oameni. Cele mai multe bănci de azi nu au casieri, manageri sau sucursale, iar datele sunt împrăştiate fără ca personalul specializat să le verifice mai întâi. Angajaţii costă bani, de care agenţiile de scoring şi companiile de creditare nu sunt dornice să se despartă. Unii oameni nu reuşesc încă să înţeleagă de ce cartea de identitate a devenit o chestiune politică atât de sensibilă şi atât de demonizată de apărătorii drepturilor cetăţeneşti. Motivul este că lumea de azi e plină de informaţii personale, iar publicul larg nu este dispus să semneze noi

documente care ne leagă de mâini şi de picioare, chiar mai mult decât suntem deja.

Introducerea cardului naţional de identitate a fost anunţată din nou într-un discurs al reginei din noiembrie 2004, iar propunerea a atras imediat critici. David Blunkett – a cărui relaţie amoroasă cu Kimberly Fortier, editoare a revistei *Spectator,* a suscitat interesul opiniei publice, atunci când informaţiile despre ea au apărut în presă – a declarat deja, într-o dezbatere a Camerei Comunelor din iulie 2002, că „este important să nu pretindem că o carte de identitate va deveni un factor cu rol hotărâtor în combaterea terorismului internaţional. Eu nu am făcut afirmaţii privind contribuţia lor substanţială în războiul antitero“. Totuşi, în vara lui 2004, pe când discursul reginei nu era încă gata, tot el a declarat public că „un card de identitate *ar* avea o contribuţie importantă la lupta împotriva terorismului“. Cum e posibil ca aceste afirmaţii contradictorii să fie făcute de un singur politician? Aproape că e un furt de identitate precum cele pe care cartea de identitate ar trebui să le combată. Desigur, era vorba de o declaraţie politică, emisă într-un context de isterie crescândă în privinţa posibilităţii unui atac terorist în Anglia.

Proiectul de lege a estimat că sistemul cărţilor de identitate va fi funcţional din 2008. Argumentele împotriva sistemului şi a oricărui alt guvern care vrea să impună un card similar este că el schimbă irevocabil – şi în rău – relaţia dintre individ şi stat. Asta înseamnă că, efectiv, va trebui să cerem guvernului permisiunea să existăm. În cazul în care nu ne vom putea continua viaţa fără să folosim serviciile publice, fără să urmărim postul de televiziune BBC, fără să mergem la spital după un accident, fără să solicităm o pensie de stat. Formula sacră a legii şi ordinii, „Inocenţii nu au de ce să se teamă“, poate fi respinsă uşor, dacă ne amintim lecţiile pe care ni le-au oferit alte sisteme computerizate ale guvernului britanic, care s-au terminat dezastruos, cum sunt Agenţia de Paşapoarte, Agenţia pentru Ajutor în Creşterea Copilului,

Biroul de Informaţii privind Infractorii – de fapt, mai toate iniţiativele guvernamentale ce utilizau computerul.

Oriunde ar fi introdusă, cartea de identitate va crea instantaneu un nou strat de birocraţie. Când îţi duci copilul la şcoală pentru prima dată sau când îţi vizitezi doctorul sau când devii membru al unui club de golf, cardul va trebui verificat de un portar, funcţionar public, care va putea să-ţi acceseze datele personale. Cartea de identitate îţi va fi cerută cu ocazia unor „evenimente" majore din viaţa ta, cum sunt momentele când soliciţi un permis de conducere, cont bancar sau paşaport; atunci, ochiul tău va fi scanat şi comparat cu datele biometrice de pe card. Trăim într-o epocă în care deja suntem pe punctul de a ne îneca într-un ocean al legislaţiei şi al birocraţiei, iar cartea de identitate va crea noi valuri uriaşe şi costisitoare. Proiectul de lege include o clauză conform căreia poţi primi o amendă deloc neglijabilă, de până la 1 000 de lire sterline, dacă omiţi să declari la poliţie că ţi-ai schimbat domiciliul. Ce se întâmplă dacă pur şi simplu uiţi s-o faci? Proiectul de lege le cere prietenilor şi vecinilor tăi să furnizeze informaţii despre tine.

Guvernul a justificat introducerea cărţii de identitate, arătând că 35% din terorişti utilizează identităţi false. Asta înseamnă că 65% din ei n-o fac. Cum îi va opri cardul pe teroriştii islamici care vin la noi, aşa, pentru a se odihni şi relaxa? Cartea de identitate ar putea, într-adevăr, să reducă fraudele financiare, însă, în marea schemă a lucrurilor, asta reprezintă mult mai puţini bani decât sunt necesari pentru a finanţa introducerea cardului, aşa că nu se poate spune că-şi va recupera cheltuielile. Guvernul estimează că instituirea sistemului va costa cel puţin două miliarde de lire sterline şi probabil, în timp, costurile vor creşte. Ministrul de Interne a afirmat în repetate rânduri că acest card va fi foarte important, punând accent pe siguranţă, protecţie, închiderea persoanelor periculoase la nevoie şi menţinerea lor sub control. Printre alte declaraţii, am fost asiguraţi

şi răsasiguraţi că sistemul va pune capăt turismului medical, cardul fiind utilizat pentru a se vedea cine este cu adevărat îndreptăţit să fie tratat de Serviciul Naţional de Sănătate. Michael Wilkis, preşedinte al Comitetului de Etică din cadrul Asociaţiei Medicale Britanice (BMA), a răspuns acestei afirmaţii întrebând: „Ce proceduri vor trebui urmate în cazul unei urgenţe, când pacientul nu are un card asupra sa? Ce implicaţii vor avea bolile infecţioase ale unor persoane care nu deţin o carte de identitate?“

E greu de înţeles de ce politicienii sunt atât de nerăbdători să impună publicului cărţi de identitate, atâta timp cât în zilele noastre toţi suntem înregistraţi, cu cele mai mici detalii, în alte părţi. Cunoaşterea înseamnă putere, iar cardul este, evident, atractiv pentru un partid care crede în conceptul de „guvernare prin sprijin reciproc“. O bază de date unică, în care întreaga noastră istorie personală este accesibilă la o simplă „citire“ a unui card poate părea o soluţie ingenioasă şi eficientă unui politician, dar şi îngrozitor de intruzivă omului de pe stradă. Dar poate însăşi denumirea „carte de identitate“ ne deranjează atât de mult. Ce trebuie să faci pentru a-i dovedi că exişti guvernului pe care l-ai ales? Adevărul este că, cel puţin în Marea Britanie, paşaportul britanic e pe punctul de a deveni întru totul o carte de identitate, numai că nu se numeşte aşa. Informaţiile care pot fi accesate graţie benzii electronice din noul document vor fi completate cu o amprentă. Paşaportul va costa 70 de lire sterline (în comparaţie cu 42 de lire, cât e acum), iar preţul i-ar putea creşte până la 85 de lire dacă guvernul va fi obligat să includă planurile sale pentru cartea de identitate în sistemul paşapoartelor. Fotografia posesorului există deja. În 2006, cel puţin 600 000 de persoane care solicitau paşaport pentru prima dată au fost intervievate de Biroul Paşapoarte, iar numărul birourilor acestui departament a crescut de la şapte la 80. Personalul este acum de 500 de ori mai numeros. Foarte puţini ştim exact ce date va conţine banda

electronică de pe paşaport. Conform Ministerului de Interne, mărirea numărului de informaţii incluse pe banda electronică este necesară pentru a combate fraudele din ce în ce mai sofisticate. Pe măsură ce ameninţarea furturilor de identitate creşte, ţări din toată lumea înăspresc măsurile de securitate a paşapoartelor. Noua bază de date a paşapoartelor se va supune Legii protecţiei datelor şi, potrivit lui Simon Davies de la Privacy International, decizia finală privind informaţiile incluse în paşaport depinde de soarta cărţii de identitate.

Probabil cea mai importantă întrebare este dacă, în schimbul acestei puteri însemnate pe care le-o oferim, putem să avem încredere în cei pe care îi votăm că vor administra sistemul de identitate cu onestitate şi eficienţă. Pot ei garanta protecţia datelor? Putem crede că ei ne vor spune adevărul în privinţa motivelor pentru care este necesar cardul? Vor înregistra oare în baza de date şi informaţii despre noi asupra cărora nu vom fi înştiinţaţi? Cum ne vom asigura că datele incorecte despre noi pot fi îndreptate?

Dacă eşti cetăţean britanic, se pare că numele tău va apărea în cel puţin 5-6 baze de date ale instituţiilor statului. Cu noile paşapoarte şi eventualele cărţi de identitate, lista lucrurilor pe care statul le ştie despre noi se va mări considerabil. Baza de date ADN a poliţiei şi cea imensă a Serviciului Naţional de Sănătate ne vor identifica după corpurile noastre sau după starea de sănătate. Cazierele noastre rămân unde au fost întotdeauna, numai că acum sunt disponibile la simpla atingere a unui buton. În ceea ce priveşte problema puştilor care trag chiulul de la şcoală şi teama generalizată de molestare a copiilor, cât va mai dura până când fiecare copil din ţară va trebui să poarte asupra sa un card şi va fi înregistrat undeva într-un computer?

Eu cred că este doar o chestiune de timp.

CAPITOLUL V

Distracții și jocuri de noroc

Companiile de supraveghere își testează în mod curent produsele în cazinouri, deoarece trișorii sunt cei mai bine pregătiți adversari de pe piață. Există o unică metodă prin care se poate garanta câștigul într-un cazinou, iar acea metodă este trișatul. Nu poți învinge sorții niciodată. Chiar dacă mai pierd din când în când câte câte un milion de dolari în favoarea vreunui miliardar nesocotit aflat în trecere, cazinourile își recuperează pierderile pe termen lung, deoarece beneficiază de pe urma a ceea ce se cheamă „avantajul casei": toate jocurile de noroc organizate de casă au de la bun început probabilitățile de partea acesteia și împotriva jucătorului. Profitul mediu al unui cazinou se situează între 17 și 18%. Legea britanică a jocurilor de noroc este una foarte strictă. „Atențiile" nu sunt privite cu ochi buni. O masă gratuită din când în când, ori o mașină cu șofer, poate un pahar de șampanie – acestea sunt permise, însă prostituatele de lux, zborurile la clasa întâi și apartamentele la hoteluri de cinci stele sunt strict interzise în Marea Britanie. În alte țări, precum cele din Orientul Îndepărtat și Africa, legislația este mai puțin severă. Unul dintre cele mai fascinante aspecte legate de industria cazinourilor este sortimentul bogat de trișori pe care i-a atras de-a lungul anilor. Câteva dintre cele mai strălucite minți din lume s-au dedicat încercărilor de a câștiga la cărți, la zaruri sau la ruletă, pentru că singurul

mod de a câştiga pe termen lung este să încalci regulile. Aceasta este o înfruntare între cei care supraveghează şi cei care schimbă puţin datele jocului.

Cea mai concisă descriere a modului cum funcţionează un cazinou este dată de Robert De Niro în filmul *Casino,* în care îl interpretează pe directorul unei luxoase săli de joc din Las Vegas. „Cum funcţionează?“, este întrebat la începutul filmului. „În primul rând, îl ai pe crupier; apoi, e inspectorul care îl supraveghează pe crupier; după aia, pit boss-ul care îl urmăreşte pe inspector; managerul de etaj care îl urmăreşte pe pit boss. Eu stau sus şi mă uit la managerul de etaj... În sfârşit, mai e şi ochiul din plafon, care vede tot.“

Pe lângă probabilităţi, un cazinou se mai bucură de alte două avantaje. În primul rând, dispune de banii necesari pentru a proteja „avantajul casei“, adică este capabil să achiziţioneze orice sistem de supraveghere cunoscut omului şi să angajeze cel mai competent personal de securitate. Apoi, dată fiind experienţa unui secol de existenţă, toate trucurile din branşă sunt bine cunoscute. Cazinourile mari din Londra aduc experţi care să-i înveţe pe angajaţii responsabili cu securitatea cum ar putea fi duşi de nas. Jucători străluciţi de cărţi, precum americanul Richard Marcus, unul dintre cei mai mari trişori din lume, care a străbătut lumea câştigând sume imense graţie mâinilor lui de aur, oferă în mod regulat prezentări private în Londra. A studiat întreg arsenalul tehnic cu care s-a confruntat, a avut nervi de oţel şi a înţeles psihologia personalului din camerele de supraveghere.

Nu poţi păcăli camera de filmat. Este singurul lucru pe care te poţi baza, fiindcă nu are inimă, nu are creier şi, mai ales, nu joacă. În mod cert, nu te poţi baza pe personal. Trebuie să accepţi faptul că tot ce poate fi făcut pentru a învinge sistemul a fost făcut deja, cel puţin o dată, şi va fi făcut din nou.

Coruperea crupierilor și a personalului de securitate s-a realizat cu succes de nenumărate ori, însă proprietarii de cazinouri învață din greșeli și implementează sisteme care să descurajeze tentativele de corupere a personalului; din acest motiv, toată lumea e supravegheată cu ochi de vultur. Multe cazinouri impun crupierilor să poarte șorțuri – nu pentru a preveni murdărirea hainelor, ci pentru a face mai dificilă strecurarea jetoanelor în buzunar. Uneori, personalul este percheziționat la sfârșitul turei, iar în unele state din SUA, jetoanele conțin dispozitive de urmărire, astfel încât șeful să știe unde îi ajung banii.

Sistemele neurale pentru depistarea și evidențierea anomaliilor din tiparele de comportament au fost utilizate pentru prima oară în Marea Britanie de Ladbrokes. Mișcările din cadrul unui joc de noroc sunt previzibile prin aceea că respectă un set de reguli. De pildă, odată încheiat procesul de pariere, nimeni nu mai poate atinge jetoanele de la masa de joc. Același lucru se aplică tuturor jocurilor, inclusiv celor de blackjack (21) sau zaruri. Un sistem neural orientat către pânza mesei de joc poate surprinde și scoate în evidență un pariu întârziat ori îndepărtarea unei sume pariate înainte ca rezultatul să fie anunțat de către crupier. De îndată ce aceasta se întâmplă, personalul de pază se prezintă la fața locului, iar jucătorul în culpă este oprit. Richard Marcus și-a luat sistemul drept aliat atunci când a descoperit că anumite combinații de culori ale jetoanelor anihilează sistemul neural într-o lumină artificială. Această descoperire i-a adus frumoase sume de bani. În cazinourile dotate cu supraveghere contra măsluirii mizelor, Marcus punea o miză și o muta doar atunci când nu câștiga. Echipa sa era formată din trei membri, cu ajutorul cărora afla instantaneu numărul câștigător la ruletă și, în cazul unui eșec, își recupera jetoanele, în mijlocul haosului creat de solicitarea de plată a câștigurilor de către ceilalți participanți la joc.

Fabricanții de echipamente au fost, de-a lungul timpului, mituiți pentru a modifica modul de funcționare al ruletei sau al

zarurilor. Cărţile se pot marca, se pot monta computere şi camere de filmare pe podea pentru a stabili avantajul casei, se pot fixa magneţi pe masa de ruletă. Dorinţa disperată de a învinge, măcar o dată, cazinoul şi de a câştiga ceva în schimbul a nimic pare să-i obsedeze pe mulţi din cei care au drept pasiune jocurile de noroc şi să planeze mereu ca o ameninţare asupra industriei. Toate cazinourile mari au luat măsuri de protecţie. Podeaua este filmată şi supravegheată 24 de ore din 24, mesele sunt testate cu cele mai performante cumpene, roţile ruletelor sunt echilibrate şi controlate periodic, pachetele de cărţi sunt livrate cu ajutorul furgonetelor securizate şi puse spre păstrare în seifuri.

Jocurile de noroc sunt un viciu. Când merge din ce în ce mai rău şi parcă eşti posedat, nu mai e vorba doar de dorinţa de a câştiga, de a deveni miliardar cu iahturi, avioane private şi femei frumoase. O miză devine ca un drog. Pentru mulţi, reprezintă o senzaţie apropiată de cea pe care o ai în timpul sexului. Un debuşeu scurt după o perioadă tensionată, care parcă nu se mai termină. Pentru unii, atracţia o reprezintă ucigătoarea aşteptare de după încheierea pariurilor, când inima îţi stă în loc – trei minute de groază, în care nici nu mai respiri, aşteptând ca bila albă să se oprească din goană în dreptul unui număr anume. Sau întoarcerea ultimei cărţi, când inima îţi bate să-ţi sară din piept şi mâinile nu se mai opresc din transpirat. Pentru alţii, rezultatul nici nu contează prea mult. Importante sunt emoţiile care însoţesc scurgerea printre degete a ultimelor rămăşiţe ale averii moştenite. Euforia jocului, a câştigului şi a eşecului, vine după ani şi ani de pariat la întâmplare, de extaz şi de agonie. De asemenea, se prea poate ca ţelul să fie câştigul. Câştigul cu orice preţ. Tocmai împotriva acestei dorinţe se înverşunează, cu toate resursele de care dispun, supraveghetorii. Personalul cazinourilor nu este angajat niciodată fără ca dosarele să fie analizate în prealabil cu cea mai mare atenţie, şi cele mai multe săli de joc recurg

la companii precum LexisNexis pentru a obține aceste informații pentru toți angajații.

Alții știu că există metode de a învinge casa. Sunt școli în America în care absolvenții de facultăți cu profil real sunt antrenați în arta de a număra cărțile la blackjack. Ai nevoie doar de multă inteligență, de o memorie redutabilă, de răbdare și de puterea de întoarce avantajul împotriva casei, prin cunoașterea întocmai a poziției fiecărei cărți din teancul crupierului. Problema derivă din aceea că există șase pachete de cărți în teanc. Pe de altă parte, „numărătorii" nu s-au născut de ieri, de azi. Aceștia joacă 21 cu o frecvență care depășește puterea de imaginație a celor mai mulți dintre noi, așa că sunt prinși și devin *persona non grata* atunci când se lăcomesc sau când pit boss-ul și supraveghetorii din camerele de deasupra îi recunosc după tiparele lor de joc. Câteodată, identificarea se realizează cu ajutorul programului de recunoaștere facială, instalat pe sistemul de supraveghere cu circuit închis. Ocazional, se poate afla dacă cineva care câștigă suspect de mult a fost vreodată evacuat din alte săli de joc.

Software-ul biometric de recunoaștere facială este utilizat în mod regulat de sălile de joc americane. Caesar's Palace din Las Vegas nu doar îl folosește, ci îi și face reclamă, iar multe cazinouri britanice l-au testat. Sistemul este foarte popular în Statele Unite, dată fiind decizia guvernului de a-l utiliza ca măsură aniteroristă, ceea ce a crescut în același timp investițiile în tehnologie. Capul securității dintr-un cazinou londonez din Curzon Street mi-a mărturisit că, în opinia sa, recunoașterea facială se realizează cu mai mult succes de către personalul angajat. „Recepționerii noștri au o memorie redutabilă și s-a dovedit că deciziile lor de a permite sau nu accesul unui jucător în cazinou sunt mult mai de încredere decât orice nouă tehnologie. Pariorii dați afară se vor întoarce, mai devreme sau mai târziu, deghizați și cu identități false. Nici un sistem de supraveghere nu va sesiza așa ceva. Noi ne bazăm pe instinctul angajatului.

Ştiu din surse de încredere că sistemul de recunoaştere facială de la Caesar's Palace funcţionează anapoda. Sunt mii de jucători, şi, chiar atunci când monitoarele indică ceva, tot trebuie să trimiţi oameni să rezolve situaţia. Nu e întotdeauna simplu şi, în opinia mea, nu e o tehnologie în care să te poţi încrede."

Primul lucru de care îţi dai seama când intri într-un cazinou este că eşti supravegheat, şi eşti lăsat intenţionat să îţi dai seama de asta. Camerele sunt pretutindeni şi fiecare mişcare îţi este înregistrată cu imagini de cea mai înaltă calitate. Peste tot e câte un pit boss sau manager de etaj – bărbaţi cu privirea rece, îmbrăcaţi la patru ace, care supraveghează jocurile şi jucătorii. Crupierii îşi fac treaba cum pot mai bine, încercând în acelaşi timp să prevină măsluirea mizelor, retragerile jetoanelor ori schimbarea poziţiei acestora. Orice joc de noroc necesită utilizarea unei anumite tehnologii de bază. De pildă, roata ruletei este verificată şi echilibrată regulat, astfel încât, atunci când se învârte, să nu existe posibilitatea de influenţare a probabilităţilor. Pachetele de cărţi îndeplinesc un standard întotdeauna acelaşi, iar jetoanele sunt imposibil de reprodus. Mişcările suspecte sunt sesizate imediat, dacă se utilizează tehnologia neurală ori dacă pit boss-ul observă ce se întâmplă. „Dar oricât de performantă ar fi tehnologia utilizată, tot ai nevoie de oameni la faţa locului", susţine sursa mea de pe Curzon Street. „Sistemul neural este impresionant şi te anunţă instantaneu, dar tot e nevoie să ajungi la sursa problemei în timp util. Oricât de eficient ar fi modul de comunicare, aceasta se poate dovedi foarte dificilă într-un cazinou aglomerat."

Desigur, industria nu e ferită de anomalii. De pildă, în Marea Britanie, echipamentul folosit de cazinourile din provincie este adesea inferior celui de ultimă oră din Crockfords sau Les Ambassadeurs. Cazinourile cu ştaif din Londra utilizează cel mai bun echipament de pe piaţă, solid şi rezistent la uzură, cu părţile din lemn măiestrit lucrate şi incrustate, cu axul şi

rulmenții gândite și puse în practică de meșteșugari adevărați. De cealaltă parte a balanței, în orașele de provincie, cu cote inferioare, în care jucătorii nu se așteaptă să găsească luxul cazinourilor din alte locuri, standardele dotărilor din sălile de joc lasă adesea de dorit. În 2004, patru oameni au devenit indezirabili în cazinourile din Midlands, după ce au pus cu succes în practică „schema grăsanului". Deși camerele de supraveghere au înregistrat după un timp incidentul, detectarea acestuia a durat ceva. Schema necesită trei jucători. Un bărbat solid apare, cu un număr mare de jetoane de valoare mică, și se așază la capătul mesei, cât mai departe de ruletă posibil. Cei doi complici, a căror prezență bărbatul o ignoră, încep să joace, observând cu atenție tiparul numerelor, în timp ce ruleta este în mișcare. În prealabil, cei trei au putut observa că suprafața pe care ruleta se află și ruleta însăși sunt atașate unei plăci lemnoase nu foarte stabile, a cărei suprafață poate fi modificată de o persoană având o greutate considerabilă, formând astfel un unghi menit să influențeze ruleta.

De-a lungul câtorva ore în care grăsanul și-a odihnit burdihanul la capătul mesei, cei trei au putut stabili un tipar de modificare a unghiului favorabil lor. Odată stabilită tehnica eficientă, este vital ca trișorii să nu devină prea lacomi. Tiparele de pariere, câștigurile și pierderile sunt permanent înregistrate și transformate în grafice în cazinouri, oricât de mici ar fi aceste cazinouri. Dacă modul de joc sfidează în mod suspect avantajul casei, atunci ceva e în neregulă și supraveghetorii intră în alertă. Cei trei nu au stat locului, căutând permanent alte cazinouri cu dotări vulnerabile în fața unui supraponderal. Pe măsură ce și-au perfecționat tehnica, au începutsă câștige tot mai mult. Au fost prinși în Leeds de un supraveghetor vigilent, care, când și-a dat seama din înregistrările camerelor cu cine are de-a face, a instalat o cameră cu lentile din fibră optică pe un pilon din apropierea mesei. Desigur, nu a obținut cine știe ce dovadă (rareori se

găsesc astfel de dovezi), însă industria răspunde întotdeauna la fel atunci când are certitudinea că unii din clienţii lor umblă cu ocaua mică. Îi filmează, îi dau afară şi le interzic să revină, scriu o descriere a escrocheriei şi o răspândesc în întreaga branşă, dimpreună cu fotografiile celor implicaţi.

Arhivele celor mai multe companii de jocuri de noroc sunt meticulos organizate. Aşa şi trebuie, pentru că, prin forţa lucrurilor, la mijloc sunt banii acţionarilor, deci o chestiune sensibilă pentru ei. Crockfords, de pildă, ţine înregistrări privind orice jucător suspect, devenit *persona non grata* oriunde în lume.

Personalul de securitate angajat în branşă este intransigent şi calificat corespunzător. Şeful securităţii de la Crockfords s-a alăturat companiei după ce a ieşit la pensie din cadrul poliţiei metropolitane ca superintendent-şef, al doilea grad ca importanţă în cadrul poliţiei britanice, unde era şeful Diviziei Cluburi şi Vicii la secţia din Charing Cross. Ajutorul său este fostul său subaltern, un inspector-şef care derula operaţiuni împotriva cluburilor din West End. Aceleaşi standarde nu sunt, însă, valabile pentru toată industria. Unii angajaţi au mai multă experienţă decât alţii. Supraveghetorii au experienţă în legile care guvernează jocul în sine. Le-au văzut pe toate, din acest motiv au fost angajaţi. De-a lungul carierei lor de oameni ai legii, ei îi vor fi băgat la răcoare pe unii dintre cei mai abili escroci.

Jocurile de noroc sunt o afacere globalizată. Cei împătimiţi călătoresc în lumea întreagă doar pentru a juca. Duc o viaţă de huzur şi caută acele jocuri unde îi găsesc pe alţii asemenea lor. Sunt jucători de cărţi, cel mai adesea de pocher sau de black jack, şi preferă locurile unde poturile sunt nelimitate, iar directorii – persoane discrete. Modurile de a trişa sunt la rândul lor internaţionale, deoarece escrocii trebuie să găsească permanent ţări unde încă nu sunt cunoscuţi şi pot să o ia de la zero. Industria cazinourilor se află în plină creştere, săli imense deschizându-se în Australia, Africa de Sud şi Orientul Îndepărtat. Introducerea

unei noi tehnologii înseamnă noi dificultăţi pentru industrie. Cazinourile britanice şi americane, deşi au considerat identificarea prin frecvenţe radio (RFID) ca pe un nou mod de a supraveghea traseul jetoanelor şi de a preveni utilizarea impropriei a bunurilor proprii ori spălarea de bani, nu s-au grăbit să investească în coduri de bare radio, din cauza costului ridicat al acestei tehnologii. Pe de altă parte, americanii şi-au instalat în cazinouri toate sistemele tehnologice cunoscute omului, inclusiv pe cele de urmărire. Trişorii nu se sfiesc să utilizeze potenţialul oferit de mijloacele electronice pentru a transmite, în mod discret, informaţii pe distanţe scurte. La începutul lui 2005, opt infractori thailandezi au fost arestaţi în Popiet, un sat de vacanţă din Cambodgia, apropiat de graniţa cu Thailanda şi de oraşul Chiang Mai. Ei fuseseră prinşi după ce au câştigat, cu sprijinul unui dispozitiv electronic, 90 de milioane de bath (peste 1,2 milioane de lire sterline) la blackjack, în cazinoul Star Vegas. Personalul de securitate a declarat că aceştia montaseră microcipuri în jetoanele de joc, ceea ce le-a permis să scaneze cărţile şi să transmită mai departe datele către un laptop dintr-o cameră de hotel. Complicii aflaţi acolo îi contactau apoi pe telefonul mobil, oferindu-le, prin mesaje codate, informaţii despre cărţile de joc.

Importanţa ochiului electronic este greu de estimat, deoarece el are preponderent un rol preventiv. Americanul Richard Marcus a trăit ani buni de pe urma escrocheriei sale la ruletă, parierea pe coloana cunoscută drept „19-le prin 36“. Aceasta nu era niciodată sesizată de camere, deoarece parierea se făcea cât mai departe posibil de crupier şi, de îndată ce bila albă se oprea în dreptul unui număr, Marcus urma să ascundă miza, în cazul în care aceasta includea, printre celelalte jetoane, unul cu valoare mare, sau să o păstreze, dacă suma pariată nu era una semnificativă. El şi-a botezat schema „Savannah“ şi plănuia să joace o „Super Savannah“ la cazinoul Horseshoe din Las Vegas, către sfârşitul carierei sale. Dacă aceasta s-ar fi dovedit

de succes, i-ar fi adus 1 050 000 de dolari. Marcus a renunţat, însă, dat fiind că şansele la ruletă de a ghici numărul câştigător sunt de 37 la 1 şi ar fi trebuit să parieze 30 000 de dolari pentru a câştiga. Ar fi trebuit şi să recurgă la măsluirea mizei, dar poate ar fi fost nevoit să o facă de mai multe ori. Ştia că, dacă i-ar fi mers, cei de la supraveghere ar fi început să se uite cu atenţie pe casetele cu înregistrări şi că astfel ar fi fost prins. Aşa că a ieşit la pensie, deşi nu poţi să nu te întrebi: „S-a retras cu adevărat?“ sau „E într-adevăr atât de priceput pe cât susţine că este?“

Utilizarea RFID, deşi a dat amploare încercărilor de identificare a trişorilor din industria jocurilor de noroc, este implementată cu mari dificultăţi în Marea Britanie, din cauza costurilor pe care le presupune. Un grup de patru albanezi a fost arestat la Ritz Casino din Londra în 2004, după o plângere a personalului de supraveghere. Câştigaseră între 2 şi 3 milioane de lire sterline, folosindu-se de un celular modificat şi de tehnologia laser pentru a influenţa modul de funcţionare al ruletei. Poliţia nu a putut dovedi nici ce s-a întâmplat, nici că s-a întâmplat ceva. Telefonul mobil a fost demontat şi examinat de specialiştii de la Nokia. Arestarea a fost în principal rezultatul schimbului de informaţii cu cazinouri din Franţa şi Italia, de unde est-europenii plecaseră, de asemenea, cu buzunarele burduşite. Convinşi de faptul că fuseseră traşi pe sfoară, cei de la Ritz au refuzat să plătească sumele câştigate, însă investigaţia oficială s-a stins de la sine, când anchetatorii nu au reuşit să prezinte nici măcar o probă fizică a producerii infracţiunii. Suspiciunile nu cântăresc prea mult într-un tribunal, aşa că, după şase luni de inactivitate şi frustrări, jucătorii şi-au primit banii. Au părăsit ţara şi, fără doar şi poate, acum golesc seifurile cazinourilor undeva prin Orientul Îndepărtat.

Jocurile de noroc atrag personalităţi puternice. Pentru a fi bun, trebuie să ai nervi de oţel, să-ţi meargă mintea, să ştii care-ţi

sunt şansele şi să ţii pasul cu noile tehnologii, mai ales acum, în epoca microcipurilor şi a sistemelor sofisticate de supraveghere. Pentru a fi un jucător excelent, trebuie să fii 100% hotărât să câştigi şi să ai un orgoliu ieşit din tipare. Donald Trump, proprietarul Turnurilor Trump din Atlantic City, vrând să deţină cazinoul aflat la cea mai mare înălţime din America, s-a confruntat cu următoarea piedică: hotelul său avea doar 48 de etaje, un număr insuficient pentru ambiţiile sale. Astfel încât a modificat modul de funcţionare al liftului, iar acum etajele de la 2 la 9 lipsesc, pentru ca el să se poată lăuda cu un cazinou la etajul 54. Asta înseamnă enorm pentru el.

Detectarea utilizări „numărării" la blackjack se face prin verificarea computerizată a tiparelor de joc. Şcolile unde se predă „numărarea" la blackjack se mută din hotel în hotel, deghizate în cursuri de contabilitate. Tarifele pot ajuge la 15 000 de lire sterline pentru un curs de două săptămâni, şi cursanţii fac grosul muncii, de-a lungul a zece zile de dificil calcul matematic şi de practică. O şcoală cu renume în zona Las Vegas predă de asemenea măsluirea mizei şi cursuri de „mână uşoară". Un „numărător", odată ce şi-a dat seama unde se află cărţile mai mari, pune o unică miză cu valoare mare înainte de a se retrage. Potrivit unui responsabil cu securitatea, detectarea se poate realiza numai prin intermediul personalului, care l-ar putea recunoaşte pe „numărător" şi prin stilul său de joc. Unele metode nu pot fi surprinse de camerele de supraveghere, ci numai de sistemele de calcul matematic al tiparului de joc.

În ceea ce priveşte mijloacele de supraveghere ale cazinourilor, frapează faptul că, în lipsa unui sistem neural, deoarece numărul de camere care înregistrează toată activitatea din sală este prea mare, nu toate pot fi privite. Arhivele televiziunii cu circuit închis sunt examinate, de regulă, numai atunci când se înregistrează probleme, iar crupierul crede că are de-a face cu o escrocherie. Măsluirea mizei la blackjack este probabil cea

mai iscusită metodă, se cere a fi executată rapid, dar va fi pusă în aplicare la nesfârşit, atâta timp cât jocul are loc în cazinouri. Odată depistată de crupier, va fi confirmată de înregistrări, aşa că toate eforturile trebuie concentrate în direcţia adormirii vigilenţei personalului. Sunt şapte secţiuni de joc la masa semicirculară de blackjack. Crupierul stă cu faţa la jucători, în centru, în spatele semicercului. Măsluirea mizei necesită o mişcare ritmică simplă. Jucătorul se aşază la masă în timp ce crupierul strânge cărţile, după plata pariurilor câştigătoare. Mai întâi, el plasează trei jetoane roşii de cinci lire în poziţia din extrema dreaptă a crupierului. Asta presupune ca, după jucarea mâinii, jucătorul să fi fost ultimul care a pariat şi să fie primul plătit în caz de câştig. Sau primul căruia i se iau jetoanele în cazul în care pierde. În timp ce se aşază, pune cinci jetoane negre de 50 de lire sterline pe pânza verde, în dreptul său, şi le acoperă cu mâna dreaptă, astfel încât nimeni altcineva din cazinou să nu le vadă. Între degetul mare şi cel arătător ale aceleiaşi mâini, el ţine două jetoane „de mişcare". În buzunarul din stânga are alte două duzini de jetoane roşii. Cărţile le joacă cu mâna stângă, lipite de stofa mesei, iar atunci când se ridică, strecoară cărţile sub jetoanele roşii. Dat fiind că joacă în extrema dreapta a crupierului, la sfârşitul mâinii el nu va putea fi văzut de restul celor de la masă. Poziţia din dreapta permite formarea unui unghi mai larg între mâna crupierului şi cercul de jucători.

Jucătorul care recurge la o astfel de escrocherie evită cu orice preţ opţiunea de a-şi dubla miza, deoarece nu doreşte să se afle într-o situaţie de verificare a mizei iniţiale, când crupierul îi poate număra din nou jetoanele. Cărţile au fost strecurate sub cele trei jetoane, jocul îşi urmează cursul corect, iar trişorul pierde. Folosindu-şi doar mâna stângă, el mai ia trei jetoane din buzunar şi le plasează în extrema stângă a cercului de pariuri, din nou lângă mâna dreaptă a crupierului. Îşi păstrează mâna dreaptă pe masă. Câştigă următoarea mână cu o pereche de

regi, în timp ce crupierul şi unul sau doi dintre jucători depăşesc pragul de 21. Crupierul întoarce cărţile şi plăteşte imediat suma corespunzătoare celor trei jetoane roşii. În timp ce el se întoarce către ceilalţi jucători, trişorul retrage cele trei jetoane iniţiale pe care pariase, în timp ce, cu mâna dreaptă, strecoară două jetoane negre de 50 de lire sterline sub cel roşu de deasupra, plasându-le exact acolo unde fuseseră jetoanele lui iniţiale. Cu aceeaşi mişcare, scapă cele trei jetoane roşii în buzunarul din stânga al sacoului, atenţionându-l cu mâna dreaptă pe crupier: „Nu te supăra, cred că nu mi-ai dat cât trebuie“, răsturnând pe masă turnuleţul cu două jetoane negre şi unul roşu.

Când managerul de etaj se prezintă la faţa locului, are în faţă miza de 205 lire sterline, cu jetoanele negre de pe masă. Am văzut cu ochii mei cum se execută această manevră pe televiziunea cu circuit închis şi nu am putut-o depista, date fiind relaxarea şi viteza cu care a fost făcută. Este o îmbinare de dexteritate şi de cunoaştere a psihologiei. Nici supraveghetorii nu au depistat-o decât la câteva săptămâni după ce a avut loc. Jucătorul a avut ghinion şi a fost pus pe lista neagră. Când va mai dori să joace, va trebui să se întoarcă în Statele Unite, adică acolo de unde a venit.

Cum jocul de zaruri utilizează serviciile a doi angajaţi, el necesită colaborarea a trei trişori. Masa este mai mică, iar crupierii – mai aproape de jucători şi mai vigilenţi. Dacă cel care aruncă zarurile nimereşte un 7 sau un 11, a câştigat. Un 2, un 3 sau un 12 înseamnă înfrângere. În orice altă situaţie, corespunzătoare unor „puncte“, zarurile trebuie aruncate din nou, până la un 7 câştigător. Dacă 7-le iese primul, jucătorul pierde, iar crupierul se alege cu jetoanele. Cele mai multe mese de zaruri sunt atent supravegheate, dat fiind caracterul haotic al acţiunilor care însoţesc jocul.

Cei trei trişori de la un joc de zaruri sunt Pariorul, Revendicatorul şi Detectivul. Pariorul pune la bătaie trei jetoane roşii.

În cazul în care câştigă, el schimbă cele trei jetoane cu altele „de mişcare“ – două vişinii şi unul roşu deasupra. Se foloseşte de ambele mâini, ridicând miza iniţială cu stânga şi înlocuind-o, instantaneu şi exact în acelaşi loc, cu dreapta. Mişcarea se cere a fi continuă şi rapidă. Odată efectuată substituirea, intră în joc Revendicatorul, care aşază un turnuleţ „de rezervă“ cu jetoane vişinii la marginea mesei, în sectorul destinat mizelor. Crupierul, care anunţă rezultatul aruncării, şi supraveghetorul aşezat între jucători, al cărui rol este acela de a observa cu atenţie desfăşurarea jocului şi împărţirea câştigurilor, nu îl vor fi observat pe Revendicator până când acesta nu începe să protesteze că nu a fost plătit îndeajuns. Motivul acestei mişcări este că Pariorul a tot mizat constant, până la acest joc, câte 15 lire sterline. Dacă el ar anunţa deodată un pariu câştigător de 2 005 lire sterline, ar suscita suspiciunea angajaţilor cazinoului. Un jucător nou care ar face asta ar fi mai uşor de acceptat.

Angajaţii cazinoului londonez cu care am discutat au căzut de acord asupra faptului că sistemele neurale oferă unica soluţie viabilă la măsluirea mizelor, deoarece atrag instantaneu atenţia asupra incidentului. Pentru sistem, mişcările din jurul unei mese de joc nu au nici o valoare, cu excepţia situaţiei în care toate camerele care înregistrează jocul sunt acoperite cumva, ceea ce este foarte greu de realizat. Masa de zaruri este, la fel ca şi cea de ruletă, una cu foarte multă mişcare, şi, chiar cu doi angajaţi la masă, o substituţie se poate realiza fără să bage cineva de seamă. Prin natura sa, jocul este unul rapid, cu un ritm al său. Orice decizie a unui responsabil cu securitatea de a nu accepta un pariu este dificil de luat. Mai greu cântăresc motivele pentru care cazinoul mai degrabă ar plăti şi jocul ar continua. Însă cea mai mare greşeală a trişorilor ar fi să se lăcomească şi să încerce din nou.

Cel de-al treilea membru al echipei este Detectivul, care trebuie să se asigure că în zonă nu se mai află şi alţi angajaţi

însărcinaţi cu securitatea ai cazinoului şi că pit boss-ul nu urmăreşte jocul. Echipele de profesionişti au un limbaj prin semne propriu, iar cei doi jucători care au făcut schimbarea stau tot timpul cu ochii pe Detectiv. Acesta poate utiliza coduri precum un strănut sau un semn cu ochiul pentru a amâna manevra. În caz de nevoie, îi poate ajuta pe Parior şi pe Revendicator să părăsească în grabă cazinoul. Detectivul nu trebuie să scape din ochi atitudinea personalului şi să aprecize vizual întreaga atmosferă din sală.

Aici sistemul de televiziune cu circuit închis devine neputincios. Pe bună dreptate, cazinourile acordă o importanţă aparte căilor de ieşire din clădire, deoarece pe acolo nu numai jucătorii, ci şi banii părăsesc sala. Nu doar asociaţii, ci şi clienţii preferă să ştie că este imposibil ca o şleahtă de haidamaci să blocheze uşa şi să înceapă să îi scuture de bani. Problema sistemelor de supraveghere este că ele nu pot prezice ceea ce urmează să se întâmple: ele înregistrează, nu fac previziuni. Sistemele neurale de ultimă oră pot ajuta privitorul să ia o decizie în legătură cu o situaţie complicată, însă întâmplările se succed al naibii de repede în sala de joc, mai ales dacă trişorii au şi o strategie de ieşire. De obicei, există o singură cale de acces în clădire. Dacă situaţia devine critică, echipa va face tot posibilul să ajungă la recepţie şi de acolo să iasă în stradă, unde cei trei se pot despărţi şi pot fi în siguranţă. Dacă este prins şi îşi ştie meseria, un jucător profesionist nu va ciripi nimic până când nu este eliberat sau îşi poate suna avocatul. Dar dacă scapă şi îl ţin nervii, trişorul mai poate sta pentru un ultim joc, punând ca miză un jeton roşu şi două violet şi plecând apoi, fără a mai aştepta deznodământul. Aceasta l-ar face pe supraveghetor, care poate şi-a dat seama că a fost fraierit, să se simtă mai bine şi să uite ceea ce tocmai s-a petrecut.

Pe de altă parte, se prea poate să nu o facă.

Capitolul VI

Aude-tot, vede-tot

Pentru oameni ca noi, spionii sunt nişte creaturi fascinante. Îi asociem cu un stil de viaţă exotic şi îi invidiem pentru abnegaţia cu care, calm şi discret, îşi văd de treaba lor, apărând interesele naţionale. Însă comunitatea agenţilor secreţi este un mecanism uriaş şi greu de manevrat, care se infiltrează în toate colţurile lumii noastre. MI5, oficial cunoscut pur şi simplu ca „serviciul de securitate", se află în linia întâi a luptei împotriva terorismului din Marea Britanie şi este în plin proces de dezvoltare a unei reţele de birouri regionale şi de recrutare a o mie de ofiţeri noi. MI5 este puternic, dar nu este corect să ne referim la el ca la o organizaţie de poliţie secretă, deoarece nu are puterea de a aresta. Pentru asta se bazează pe poliţie şi departamente precum Vamă şi Accize. Cu toate acestea, MI5 exercită o putere imensă, putând pătrunde peste tot şi instala microfoane după bunul plac. Niciodată până acum serviciile secrete nu au dispus de o asemenea putere. Şi, desigur, „umbrele" autohtone nu sunt singurii agenţi de informaţii care operează în ţară – mai avem şi spioni străini. Americanii adună informaţii despre telecomunicaţii, iar francezii nu îi scapă din ochi pe teroriştii „locali" – atât ai noştri, cât şi ai lor. Spionajul n-a fost niciodată atât de multinaţional şi atât de sofisticat tehnologic ca acum. Spionii sunt plasaţi în vârful ascuţit al aparatului de stat camuflat şi au acces la toate secretele noastre.

Oricine se afla în America în jurul datei de 11 septembrie 2001 îşi aminteşte cu siguranţă schimbarea vădită care a cuprins ţara – un amestec de şoc şi teamă. Lucram pe atunci la Universitatea din Pittsburgh. Părea că, din senin, străzile s-au golit, iar aerul curat fusese absorbit din însoritele după-amiezi de vară târzie. Ca englez, nu mă simţeam în largul meu, eram un intrus care nu avea nici un drept să se afle acolo. Preşedintele şi echipa sa dispăruseră, răpiţi de bărbaţii plini de muşchi şi cu feţe aspre, în haine de un albastru-închis şi în maşini blindate. Bush fusese dus, pe un traseu ocolit, în Omaha, Nebraska, unde era ţinut sub protecţie în Baza Forţelor Aeriene Offutt, sediul central al Comenzii Strategice. Acest centru de decizie supersecurizat fusese creat în timpul Războiului Rece. În eventualitatea unui atac cu rachete din URSS, de aici preşedintele ar fi preluat controlul asupra Comenzii Strategice a Forţelor Aeriene şi ar fi purtat un război nuclear. Ceilalţi guvernanţi erau distribuiţi în unităţile de înaltă securitate, rezistente la bombardamente, din Maryland, Pennsylvania, Virginia, West Virginia (în locuinţe subterane luxoase, în apropierea vechiului club de golf al lui Sam Snead, The Greenbrier) şi New England.

Aparent, restul naţiunii trebuia să-şi înfrunte singură soarta. Eu m-am trezit, în aeroportul din Pittsburgh, în faţa unei cozi uriaşe. Era alcătuită în cea mai mare parte din cetăţeni americani disperaţi să se întoarcă în New York – sau oriunde altundeva îşi aveau domiciliul – şi străini de pretutindeni, disperaţi, dimpotrivă, să părăsească ţara. Cozile erau vegheate de bărbaţi gigantici şi femei cu chipul împietrit – persoane însărcinate să rezolve rapid orice revoltă. Oamenii aşteptau ore întregi, nemişcaţi şi tăcuţi, demoralizaţi şi înfricoşaţi, expuşi pentru prima dată ororilor unui atac pe pământ american. În sfârşit, pasagerilor li s-a permis să se împrăştie către destinaţiile lor, atunci când a devenit clar că, în pofida ameninţării teroriste, traficul aerian trebuia cumva să continue, iar ţara începea să se

îndrepte cu paşi siguri către o fundătură (exact scopul pe care Al Qaeda sperase să-l atingă). Impactul terorii asupra Statelor Unite era groaznic de privit şi din el s-a născut o atitudine de intoleranţă impasibilă care persistă şi azi. Când s-au mai liniştit puţin apele, preşedintele a ieşit din gaura sa zăvorâtă, iar jalea după morţii din turnurile gemene s-a preschimbat în furie. Uriaşul adormit se trezise şi a descoperit că informaţiile şi cunoştinţele despre duşman erau dureros de insuficiente.

Comunitatea spionilor americani, aşa cum se prezintă ea azi, îşi are rădăcinile în Pearl Harbor. Americanii ştiau de atacul japonez, însă informaţiile în acest sens se aflau în locuri diferite şi erau „proprietatea“ unor diverse grupuri militare şi civile. Nici o agenţie de informaţii în funcţiune nu avea dreptul de a analiza materialul şi de a trage concluzia evidentă. Aşa s-a născut Agenţia Centrală de Informaţii (CIA), împărţită în două mari direcţii: Direcţia Operaţii, care colectează informaţiile, şi Direcţia Informaţii, care le analizează. Pare logic, nu? Din nefericire, nu e chiar aşa. Din 1946 încoace, au început să se dezvolte alte câteva zeci de colectori de informaţii. Agenţia Naţională de Securitate (NSA), care beneficiază de un buget mult mai mare decât cel al CIA, este responsabilă cu interceptarea transmisiunilor, cum ar fi convorbirile pe telefoane mobile şi semnalele radio. Vine apoi Biroul Naţional de Recunoaştere. Treaba lui este să adune informaţii vizuale de la avioane strategice de recunoaştere şi de la sateliţii NSA, pentru a le oferi apoi Agenţiei Naţionale de Informaţii Geospaţiale (NGA). Armata şi CIA includ, de asemenea, agenţii de colectare a imaginilor. Pentagonul răspunde de Agenţia de Informaţii pentru Apărare (DIA), cu propriul serviciu de informaţii – Servicii pentru Apărarea Umană, care, în acelaşi timp, primeşte informaţii de la CIA, NSA şi NGA. DIA are sarcina de a se concentra asupra capacităţilor militare ale inamicului – ceea ce nu este deloc uşor atunci când ai de-a face cu o organizaţie nestructurată şi

obscură precum Al Qaeda. În plus, toate forţele armate au în subordine propriile agenţii de colectare a informaţiilor, preocupate în special cu chestiuni tactice, dar care adună întâmplător tot felul de alte materiale.

Mai există şi o serie de organizaţii poliţieneşti civile care activează în domeniul colectării de informaţii. Biroul Federal de Investigaţii (FBI) se ocupă atât de contraspionaj, cât şi de impunerea legii, având şi o responsabilitate contrateroristă. Acest ultim rol al FBI prezintă o importantă contradicţie. Biroul are ca angajaţi poliţişti a căror meserie este aceea de a rezolva infracţiuni comise deja. De fapt, activitatea Biroului este evaluată după rapoartele sale cu infracţiuni soluţionate. Contraterorismul se ocupă însă cu împiedicarea producerii unor acte criminale în viitor: colectezi informaţii, le analizezi şi le prevezi efectele. Alte agenţii, precum Departamentul Alcool, Tutun şi Arme de Foc (AFT), Administraţia Antidroguri (DEA) sau Vămi şi Siguranţa Graniţelor (CBS), colectează toate informaţii, folosite pentru a înlesni arestările şi punerile sub acuzare. Departamentul de Stat răspunde de Serviciul de Securitate Diplomatică (DSS), o agenţie de contrainformaţii însărcinată cu protecţia ambasadelor SUA. Departamentul Apărării conduce Biroul pentru Planuri Speciale (OSP). Acest grup elitist al „umbrelor" este restrâns, dar puternic, şi deţine resurse considerabile. Este alcătuit din analişti reputaţi şi obţine informaţii prin secretarul apărării. OSP şi desele sale opinii piezişe au primit mai multă atenţie decât orice alt grup după evenimentele din 11 septembrie.

Se poate spune că, în 2001, cantitatea de informaţii deţinute de organizaţiile militare, de stat şi civile din Statele Unite scăpase de sub control, iar analiza acestor informaţii se apropia vertiginos de un dezastru. Nu exista o singură unitate pe teritoriul Statelor Unite în care să fie colectate, analizate şi evaluate toate informaţiile obţinute de agenţii. După tragedia de la turnurile gemene, a devenit imediat evident că excelenta idee a creării

CIA după Pearl Harbor fusese de mult abandonată. Diversele interese particulare preluaseră controlul şi „comunitatea informaţională“ se dovedea din nou un haos, în care agenţiile concurente scormoneau cu disperare după informaţii, pe care le păstrau numai pentru uzul propriu. Cunoştinţele existau, la fel cum existau motivaţia, abnegaţia şi tehnologia. În aceste condiţii, cum a fost posibil ca 19 terorişti arabi să trăiască, să se instruiască şi să acţioneze pe tărâmul libertăţii, pentru ca apoi să deturneze patru avioane şi să producă efecte atât de catastrofale?

Ca nou director al Departamentului Naţional de Informaţii, John Negroponte avea la dispoziţie un buget de 40 de miliarde de dolari. El avea sarcina de a administra şi de a armoniza activitatea celor 15 agenţii de informaţii finanţate de către stat care operează în Statele Unite şi de a întreţine contacte strânse cu agenţiile străine, în special cu cele britanice. Responsabilităţile sale au fost smulse din strânsoarea fostului secretar al apărării, Donald Rumsfeld. Negroponte, diplomat de carieră cu o experienţă redusă în lumea informaţiilor, a devenit unul dintre cei mai puternici oameni din America şi misiunea lui era de a-şi folosi abilităţile diplomatice ca să-i forţeze şi să-i amăgească pe spionii americani să coopereze, să-i încurajeze să nu se mai întreacă între ei, ci să lucreze împreună pentru binele naţiunii. Nu era deloc o misiune uşoară căci serviciile secrete americane, militare şi civile – care au fost criticate aspru de către mass-media, politicieni şi opinia publică după 11 septembrie, în special cu referire la Războiul din Irak –, riscau să nu-şi mai revină niciodată. Trei alte persoane importante au fost contactate înainte ca el să accepte funcţia, dar toate au refuzat oferta.

Negroponte s-a născut la Londra în 1939, ca fiu al unei englezoaice şi al unui magnat grec din industria navigaţiei. A crescut în Europa, dar a fost educat în New York, unde s-a stabilit familia sa după război. Şi-a încheiat educaţia absolvind Dreptul la Harvard, iar în 1960 a intrat în corpul diplomatic. A doua sa

mutare în interes de serviciu a fost ca ofiţer politic în Vietnam – „o experienţă care îţi decide cariera“, cum spunea el. Unul dintre evenimentele de care cu siguranţă îşi aduce aminte este Programul Phoenix, condus de Bill Colby de la biroul CIA din Saigon. O campanie murdară, în care trupele de asasini ai CIA au fost folosite pentru a întemniţa, intimida şi ucide membri ai guvernului condus de comunişti, constituit de Viet Cong în sudul rural al ţării. Programul Phoenix a dus la moartea multor mii de vietnamezi inocenţi, iar mişcarea pacifistă a împânzit Washingtonul cu afişe în care Colby era acuzat de crimă. În anii 1980, Negroponte a fost numit ambasador al Statelor Unite în Honduras, în timpul administraţiei Reagan, pentru ca apoi să fie acuzat că a închis ochii în faţa unor încălcări ale drepturilor omului comise de către CIA. Aceasta i-a ajutat pe rebelii Contras să răstoarne regimul Sandinista, orientat către stânga, din Nicaragua vecină. Au apărut speculaţii conform cărora el ar fi ştiut totul şi ar fi tolerat „echipele morţii“ şi Batalionul 136, o unitate militară criminală, condusă de Gustavo Alvarez Martinez, general rebel din Nicaragua, precum şi că americanii ar fi cooperat la asasinate şi torturi. Negroponte a negat toate acuzaţiile care i-au fost aduse în mass-media din America. Însă, din când în când, aceste acuzaţii continuă să iasă la iveală. De-a lungul anilor petrecuţi în America Centrală, el a adoptat cinci copii orfani din Honduras, declarând: „I-am luat sub aripa mea, deoarece ei mă vor menţine tânăr. Am decis să ne adoptăm toţi copiii din aceeaşi ţară, pentru că viaţa este şi aşa destul de complicată; nu e nevoie să o îngreunăm cu fraţi şi surori din toată lumea“.

Cariera sa diplomatică l-a purtat prin Orientul Mijlociu, Europa şi sud-estul Asiei şi a învăţat să vorbească fluent limbile spaniolă, greacă, franceză şi vietnameză. Ultimul pas în această carieră diplomatică agitată a fost postul de ambasador în Bagdad, unde a fost trimis pentru a-l înlocui pe proconsulul

american Paul Bremer. Totuşi, se pare că latura sa dură s-a mai domolit, iar activitatea sa în această ţară a fost un model de precizie în diplomaţie. Acum nu mai este văzut ca un „vultur“, ci ca un funcţionar de încredere al statului, cu o reputaţie de om care tace şi face. Susţinătorul său la Washington este Colin Powell.

Printre alte agenţii, Negroponte controla CIA şi FBI; el avea nevoie să-şi utilizeze toate abilităţile diplomatice pentru a forma alianţe între cele două. Unul dintre programele cele mai delicate pe care el trebuia să le supravegheze era CAPPSII, un program de scanare a pasagerilor iniţiat imediat după atacurile asupra turnurilor gemene – atât de sensibil şi de secret, încât, în timpul alegerilor prezidenţiale din 2004, a trebuit să fie abandonat discret şi temporar. Obiectivul CAPPSII, aşa cum a fost descris de nou-înfiinţatul Departament al Securităţii Interne, era acela de a crea „un sistem automatic capabil să integreze şi să analizeze simultan numeroase baze de date venite de la guvern, industria de informaţii şi sectorul privat, un sistem care să stabilească nivelul de risc estimat pentru fiecare avion de transport, pasager, aeroport şi zbor“. Altfel spus, o tentativă de a prezice şi de a împiedica potenţialii terorişti, folosind toate informaţiile pe care Departamentul şi agenţiile sale pot pune mâna.

Mulţi turişti care au avut scurte treceri prin Statele Unite în ultimii ani cunosc procedurile neplăcute necesare pentru a depăşi ghişeul de Imigrare. Procesul tinde să fie lent şi – în mod deliberat – intimidant: un fel de a ne aduce aminte că, pe tărâmul libertăţii, mârlanii sunt la putere. La fel ca majoritatea agenţiilor, Departamentul Vămi şi Siguranţa Graniţelor îşi motivează comportamentul de neam-prost, descriindu-l ca „o parte a datoriei noastre vitale de a salva vieţile americane“. Sosind recent la aeroportul Kennedy, am fost fascinat de un agent în uniformă şi înarmat, înalt, ras în cap şi cu privire de oţel, care a apărut în sală în faţa maselor ordonate de vizitatori sau turişti şi

l-a apostrofat cu voce tare pe un tânăr care avusese curajul să-şi folosească telefonul mobil în timp ce aştepta să fie evaluat la ghişeu. Aşteptasem până atunci mai bine de o oră şi am fost obligaţi să-l ascultăm pe acel oficial urlând abuziv. Era o indicaţie clară privind dispreţul pe care îl avea pentru sărmanii călători. O fată care călătorea cu mine a fost luată într-o cameră din spate şi interogată. „Aşa mi se întâmplă de fiecare dată când vin aici“, mi-a zis ea când a apărut într-un sfârşit, arătându-mi o scrisoare de la Ambasada Statelor Unite din Londra, în care i se cereau scuze pentru o greşeală apărută în înregistrările călătoriilor ei spre şi dinspre America. „Angajatorul meu, o companie aeriană, a cerut de zeci de ori ca datele mele să fie corectate, am trimis şi scrisori ale unor avocaţi, dar funcţionarii de la Imigrare pur şi simplu le ignoră.“

În Marea Britanie, numărul tot mai mare de acte teroriste şi violente a coincis cu reducerea dramatică a eficienţei forţelor de poliţie şi o orientare corespunzătoare, foarte răspândită, către securitatea privată. Când vine vorba despre prevenirea infracţiunilor, poliţia noastră este în mare măsură inutilă. Poliţiştii sunt dezavantajaţi de birocraţie, de reglementările privind sănătatea şi siguranţa, de riscul apariţiei litigiilor, cultura compensaţiei, groaza de a nu fi acuzaţi de rasism instituţional, un volum imens de noi acte decretate ilegale de către Uniunea Europeană şi noua legislaţie a muncii, precum şi de mâna moartă a corectitudinii politice. Moralul lor este mai scăzut ca niciodată, în timp ce povara reclamaţiilor care s-au bucurat de succes, legislaţia drepturilor omului şi a protecţiei datelor întorc şansele împotriva oamenilor legii. Legea protecţiei datelor din 1998 este împărţită în 75 de secţiuni şi prevede pedepse cumplite pentru firmele şi indivizii condamnaţi că nu au respectat-o. Fiecare încălcare a acestei legi poate aduce o amendă de 5 000 de lire sterline. Ea nu a fost niciodată testată adecvat în tribunale şi metodele prin care trebuie să fie aplicată nu sunt prea clare.

Filmarea în secret a unui individ, fără înştiinţarea sa, este ilegală, iar materialele şi informaţiile obţinute pe această cale nu sunt acceptate ca dovezi în instanţă. Unităţile de poliţie apelează la firme de securitate private pentru a se proteja împotriva crimei organizate, la fel ca forţele armate, Departamentul Vamă şi Accize, cele mai multe ministere (inclusiv cel al Apărării), băncile şi toate instituţiile financiare. Poliţia britanică, în viziunea omologilor săi continentali, a degenerat într-una dintre cele mai ineficiente forţe de poliţie din Europa, dacă nu chiar din lume, în timp ce tehnologiile dezvoltate şi comercializate prin industria britanică a securităţii sunt de cea mai înaltă clasă.

Forţele de poliţie şi agenţiile de securitate folosesc în mod cumpătat supravegherea îndeaproape, deoarece e foarte costisitoare şi necesită multe resurse umane. O divizie foarte bine antrenată, ale cărei servicii sunt disponibile atât pentru poliţie, cât şi pentru serviciile secrete, şi care este identificată doar ca SO23, oferă supraveghere amănunţită, cu aprobarea unui ofiţer superior şi, în unele cazuri, a unui funcţionar de stat sau ministerial. Organizaţia de poliţie CIB, cu sediul în Vauxhall (sudul Londrei), este însărcinată cu protejarea apărătorilor legii. Ea beneficiază de fonduri aproape nelimitate, cu care să nimicească orice urmă de corupţie din forţele de poliţie. CIB are ca angajaţi ofiţeri de poliţie deseori refractari, cunoscuţi ca incoruptibili, dar îngrijoraţi de posibilitatea ca nu cumva colegii lor să afle pentru cine lucrează de fapt.

Jocheul Jamie Osborne, după ce a fost arestat sub suspiciunea de a fi aranjat nişte curse, a fost abordat de un fost ofiţer al Departamentului de Investigaţii Criminale (CID) din Thames Valley, Robert Harrington, care i-a spus că ar putea face ca investigaţia asupra sa să fie oprită, fără a i se mai aduce vreo acuzaţie. Osborne s-a dus direct la poliţie şi a fost recrutat de CIB ca *agent provocateur*, în încercarea de a-l prinde în capcană pe Harrington. În ziua anterioară vizitei lui Harrington la Osborne

acasă, SO23 instalase un cordon polițienesc în jurul căsuței jocheului și a grădinii sale cu copaci, apoi începuse să instaleze dispozitive de ascultare și camere de filmat atât în locuință, cât și pe teren. Ofițeri bine instruiți erau camuflați și ascunși în grădină, pentru protecție în fața oricărei posibile amenințări la adresa lui Osborne și a altor potențiali martori. Am avut ocazia să ascult casetele și să văd filmul înregistrat – dovezi folosite în procesul intentat lui Harrington și desfășurat la Old Bailey, Curtea Penală Centrală, unde inculpatul a fost condamnat și trimis la închisoare. Camere cu lentile din fibră optică și microfoane au fost ascunse în șemineul din sufragerie și în bucătăria locuinței, iar dispozitive au fost camuflate prin grădină. Locul a fost evacuat și apoi înconjurat cu un cordon polițienesc când au sosit experții în supraveghere; la fel s-a întâmplat după aceea, când ei s-au reîntors pentru a demonta echipamentul. Harrington a mai fost înregistrat în mai multe locuri, folosindu-se numeroase resurse umane și electronice, însă transcrierile convorbirilor și înregistrările întâlnirilor sale cu jocheul au jucat un rol crucial în condamnarea sa.

Au crescut semnificativ numărul agențiilor internaționale de informații de proporții reduse și private, precum și cererea de companii mici și discrete, precum Hakluyt, înființată de fostul angajat al MI6 Christopher James, ale cărui cunoștințe cu privire la țările în curs de dezvoltare și lumea a treia sunt legendare și care este expert în cine deține puterea în orice țară din lume și în cum poți să-ți înființezi o firmă în locuri dificile de pe planetă. Hakluyt cultivă o „aură" temerară la agenții săi, are un consiliu director înțesat de foști ofițeri de teren și un personal de tineri agenți care operează în cele mai periculoase colțuri de pe glob, unde chiar și cel mai îndrăzneț afacerist s-ar simți nesigur. Stratfor, o agenție globală de informații înființată de George Friedman, este cunoscută în Statele Unite drept „CIA-ul din umbră", deoarece combină rapoartele și analizele

media cu consultanţa de spionaj. Ea este, în esenţă, o vastă reţea colectoare de informaţii şi a ajuns să aibă o influenţă puternică în comunitatea mondială de spionaj după 9/11, graţie analizei sale pătrunzătoare asupra lipsurilor serviciilor secrete americane.

Securitatea privată a înflorit în mare parte ca răspuns la cererile industriei de asigurări ca ai lor clienţi să se protejeze singuri de spargeri, furturi şi violenţă. Industria de asigurări este capabilă să insiste ca riscurile pe care şi le asumă să fie acoperite de un nivel adecvat de măsuri preventive. Se ştie că tehnici de supraveghere sofisticate şi finanţele necesare sunt disponibile în industria securităţii de înaltă tehnologie, aflată în continuă dezvoltare. Profiturile sunt imense, iar industria nu este zăpăcită de problemele procedurale şi bugetare cu care se confruntă poliţia. Industria de securitate a devenit astfel competitivă şi inovatoare; ea înfloreşte, din moment ce operează profitabil nu doar în protecţia sectorului privat, ci şi în păzirea instituţiilor statului. Consecinţa a fost stimularea companiilor de securitate. Organizaţii precum Kroll, Control Risks şi Hakluyt s-au extins, astfel încât să opereze cu succes în comunitatea globală a agenţiilor de informaţii.

Kroll International este o agenţie de detectivi specializată în supraveghere electronică şi spionaj, condusă din New York de Jules Kroll. Compania operează în 20 de ţări, iar personalul său include aproape 20 000 de specialişti. Filialele internaţionale ale Kroll lucrează pentru guverne precum cele din Thailanda şi Africa de Sud. De exemplu, compania a sprijinit înfiinţarea Scorpionilor, o forţă de securitate internă creată de Nelson Mandela, fostul preşedinte al Africii de Sud. Serviciile Kroll sunt căutate de afaceri care necesită sfaturi de spionaj şi forţă fizică pentru a opera pe pieţe internaţionale dificile. Kroll este probabil cea mai mare şi mai sofisticată agenţie de acest gen şi şi-a clădit reputaţia că este pricepută la depistarea comorilor ascunse ale

politicienilor corupţi şi ale organizaţiilor criminale internaţionale. Serviciile sale sunt costisitoare. Compania britanică denumită Control Risks, cu sediul pe Victoria Street din City şi înfiinţată de compania turistică Hogg Robinson în 1975, oferă consultanţă în probleme de securitate corporatistă. Director este generalul Sir Michael Rose, iar agenţia sa este specializată în evitarea răpirilor şi asasinatelor, precum şi în trierea candidaţilor la un post. Control Risks are 400 de angajaţi în întreaga lume şi o strânsă colaborare cu agenţiile de securitate din Marea Britanie, pentru a proteja interesele comerciale naţionale.

Pe lângă serviciile de securitate intensivă cu efectiv specializat, care operează mai ales „la sol", guvernele din întreaga lume au început, după 9/11, să aloce bugete uriaşe pentru monitorizarea şi interceptarea comunicaţiilor electronice. În Statele Unite, interceptarea şi interpretarea semnalelor de către Departamentul Justiţiei, FBI şi Administraţia Antidroguri îşi fac simţită prezenţa în toate formele de sisteme comunicaţionale, incluzând acum accesul la internet de bandă largă şi telefonia prin Voice Over IP (VOIP). Cetăţenii care pălăvrăgesc la telefon, navighează pe internet sau se angajează în tranzacţii online obişnuite lasă în urma lor, fără să-şi dea seama, o dâră de detalii personale care sunt automat capturate şi reţinute în „jurnalele" computerelor. Tehnologia care face posibil acest lucru e într-adevăr uimitoare şi poate apărea în cele mai neaşteptate locuri.

Baza militară Menwith Hill din North Yorkshire stă sub auspiciile Agenţiei Naţionale de Securitate (NSA) şi nu emite nici o pretenţie la vizibilitate sau publicitate. Activitatea sa este fără reţineri neprietenoasă, răspunzând doar în faţa preşedintelui Statelor Unite şi a consilierilor săi pe probleme de securitate naţională. Menwith Hill reprezintă interfaţa dintre Armata americană şi spionajul purtat din spaţiu, fiind capabilă să intercepteze orice semnal sau conversaţie din Europa, Africa de Nord şi Asia de Vest. Cu cât afli mai multe despre staţia de la Menwith

Hill, cu atât te enervezi mai tare. Ea reprezintă o piesă importantă de armament de război, ascunsă în nordul Angliei, şi unul dintre locurile cele mai secrete de pe glob. Fără cel mai înalt nivel posibil de transparenţă, nimănui nu îi este permis accesul dincolo de porţi. Americanii nici măcar nu recunosc că staţia există şi refuză să lase orice vizitatori, inclusiv membri ai Parlamentului naţional sau ai Parlamentului European, să intre aici, chiar şi în ocazii oficiale. Alice Mahon, membră a Parlamentului din partea laburiştilor, a spus în faţa camerelor că nici o persoană preocupată de libertăţile cetăţeneşti nu poate ignora Menwith Hill. În pofida numeroaselor tentative de a primi răspunsuri la întrebările ei, este evident că baza militară nu răspunde în faţa membrilor Parlamentului britanic şi, ca atare, nici în faţa poporului britanic. Deşi este o staţie de supraveghere americană, în 1996 ea a fost inclusă, prin denumire, în Forţele Aeriene ale Marii Britanii, în încercarea de a camufla ce reprezintă această puternică resursă militară. Oricum, ea nu este singura în această situaţie: există staţii similare, chiar dacă mai mici, în Australia şi Austria.

Baza militară este imposibil de ascuns, nu o poţi îngropa sau muta sub pământ. O zăreşti la orizont atunci când laşi în urmă Harrogate pe autostrada 59 şi pătrunzi în Yorkshire. De la distanţă, pare o colecţie de „cupole" emisferice, mari şi albe, aşezate în ceea ce fusese odinioară o liniştită regiune necultivată. Domurile conţin „farfurii" de recepţie a informaţiilor transmise de sateliţi şi sunt înconjurate de clădiri „întărite" (rezistente la bombardamente). Menwith Hill este cea mai mare staţie de monitorizare electronică din lume şi acolo lucrează 1 200 de civili şi militari americani. Administraţia Naţională pentru Aeronautică şi Spaţiu (NASA), care controlează baza, a mai angajat un număr limitat de civili britanici, verificaţi cu atenţie, din Sediul Comunicaţiilor Guvernamentale (GCHQ). Baza a crescut de-a lungul anilor, iar puterea şi importanţa de care se bucură sunt

subliniate de închiderea celorlalte stații conduse de NSA din Marea Britanie. Noua ei destinație oficială, de Centru Operațional pentru semnale de spionaj (SIGINT), responsabil cu conducerea de la distanță a stațiilor automate de colectare a informațiilor, subliniază importanța strategică a bazei.

Motivul pentru care acest memento fățiș al lumii pline de pericole în care trăim mă calcă pe nervi este faptul că baza interceptează tot „traficul" informațional care intră în, iese din sau trece prin Marea Britanie și care are ca origine sau destinație Asia de Vest, Africa de Nord și Europa. Baza este de importanță vitală pentru americani, deoarece sateliții poziționați astfel încât să recepționeze comunicațiile din aceste regiuni sunt „vizibili" din Menwith Hill, dar nu și din Statele Unite. „Traficul" include toate apelurile pe telefonul mobil, mesajele pe mobil și prin satelit, e-mailurile, faxurile, semnalele radio și orice alt tip de comunicare electronică cunoscut omului. Dacă un semnal trece printr-un cablu sau printr-un releu radio ori satelit, stația îl poate recepționa, analiza, procesa și retransmite automat către Statele Unite.

Stația de la Menwith Hill a jucat un rol major în invadarea Irakului din 2002, interceptând și transmițând informații de comandă. Războiul a fost purtat de americani în primul rând ca un război spațial, în care aliații puteau folosi 50 de sateliți care să sprijine eforturile militare britanice și americane; 27 de sateliți de poziționare globală au fost utilizați pentru a detecta amplasarea unităților și țintelor operațiunilor speciale, iar restul pentru a transmite comunicații și comenzi și pentru avertismente privind atacuri cu rachete, tipare de condiții meteorologice și multe altele. Generalul Judd Blaisdell, directorul operațiunilor spațiale din cadrul forțelor aeriene americane, a afirmat că în jur de 33 600 de persoane, lucrând în 36 de stații SIGINT din întreaga lume, au fost implicate în activități de tipul „război spațial". Supravegherea prin satelit a fost susținută cu date oferite

de AWACS (mari aeronave de comunicaţii ce rătăcesc la „marginea“ spaţiului) şi de spionajul uman.

Sistemele nu erau în nici un caz ireproşabile. Unele rachete Tomahawk şi-au ratat cu mult ţinta în timpul invadării Irakului, iar lungimea de bandă-radio disponibilă s-a dovedit a fi inadecvată. Ultimul război din Irak a reprezentat o rafinare a tehnicilor utilizate în Războiul din Golf din 1991. Toate bombele şi armele inteligente erau controlate de sateliţi spaţiali de poziţionare globală şi acum este evident că sistemele spaţiale sunt cheia viitoarei puteri militare americane. La sfârşitul acţiunilor militare din Irak, în aprilie 2003, vorbind la inaugurarea celui de-al 614-lea escadron de spionaj spaţial, la baza aeriană Vandenberg din California, comandantul locotenent-colonel Earl White a remarcat că folosirea tehnologiei spaţiale fusese un avantaj major în război. „Fără spaţiu, revenim la al Doilea Război Mondial, a zis el. Oricine vrea să ne înfrunte va trebui să ne înfrunte în spaţiu.“

Baza de la Menwith Hill a reprezentat o importantă valoare militară în timpul ambelor războaie împotriva Irakului. Ei îi revine marea responsabilitate de a intercepta şi transmite informaţii de spionaj militar şi de comandă, pe lângă funcţiile sale de a obţine date sau de a culege şi analiza informaţii de spionaj civil şi comercial. Rolul său nu poate decât să crească, pe măsură ce America dezvoltă mai multe sisteme de luptă cu baza în spaţiu. Staţia de la Menwith Hill acoperă o suprafaţă de aproximativ 20 de acri şi controlează 56 de sateliţi dintr-o serie cunoscută drept „The Runway“ („Podiumul“), care operează în linie de la est la vest, la extremitatea sudică a bazei. În prezent, baza operează două sisteme: „Silkworth“ şi „Moonpenny“. Sistemul „Silkworth“, operat dintr-o clădire mare şi joasă din centrul bazei, găzduieşte o reţea de computere ce monitorizează sateliţii staţionaţi deasupra Ecuatorului, unde interceptează transmisiuni radio la distanţă mare de la ţintele din Eurasia şi le retransmit

către bază. Tehnologia permite personalului să asculte mesaje și conversații dintre indivizi și companii din Orientul Mijlociu și Europa. Ele sunt retransmise de sateliții Mercury, Magnum și Orion (mai avansat). Acești sateliți, la fel ca aproape toți sateliții moderni de comunicații, sunt „geosincroni" – asta înseamnă că rămân într-o poziție fixă în raport cu Pământul. Datele sunt descărcate și retrimise pentru analiză în Yorkshire, unde sunt sortate după criterii speciale într-o unitate subterană, protejată împotriva radiațiilor, numită „Steeplebush II".

Operațiunile speciale „Moonpenny" sau sistemele „Sprinkler" („Stropitoare") interceptează și recepționează comunicații neautorizate prin satelit din alte țări. Ele constau dintr-o serie de terminale de interceptare, programate să adune semnale de la sateliții de comunicații naționali și internaționali aflați sub controlul altor state (inclusiv „Arabsat" și „Intelsat"). Amploarea procesului de colectare este impresionantă. NSA are ca obiectiv strângerea tuturor comunicațiilor internaționale și a majorității celor naționale. În 1992, sistemul intercepta 2 milioane de mesaje pe oră, dintre care toate, în afară de vreo 13 000, erau ignorate înainte de a filtrate până la a se ajunge la cele 2 000 care satisfăceau criteriile pentru a fi transmise mai departe. Acestea din urmă erau reduse treptat, rezultând în final 12 comunicații care erau selectate și analizate de experți. Acum 15 ani, stația Menwith Hill intercepta anual 17,5 miliarde de mesaje, dintre care vreo 17,5 milioane puteau fi analizate.

Echelon este un sistem global de interceptare, administrat și de NSA, care captează și analizează în principiu orice apel telefonic, fax, e-mail și mesaj telex trimis oriunde în lume. Este operat în colaborare cu GCHQ din Cheltenham, Instituția pentru Securitatea Comunicațiilor (CSE) din Canada, Direcția pentru Apărare și Securitate (DSD) din Australia și Biroul General pentru Securitatea Comunicațiilor (GCSB) din Noua Zeelandă. Aceste organizații sunt reunite printr-un acord din

1948, UKUSA, ale cărui prevederi rămân încă secrete. Potrivit unei investigaţii a Comisiei Uniunii Europene din 2001, sistemul Echelon furnizează analiştilor britanici şi americani date colectate de 120 de sateliţi-spion. Acest lucru înseamnă că, în fiecare minut al fiecărei zile, sistemul poate procesa 3 milioane de comunicaţii electronice. Proiectul Echelon e simplu; el interceptează staţii din întreaga lume. Captează întreg traficul de comunicaţii prin satelit, microunde, telefoane mobile şi fibre optice, apoi procesează informaţiile prin intermediul computerelor de la NSA, care includ programe avansate pentru recunoaşterea vocii sau recunoaşterea optică a caracterelor. Personalul NSA mai caută cuvinte sau fraze de cod (aşa-numitul „dicţionar" Echelon), care determină computerul să marcheze mesajul, pentru a fi înregistrat şi transcris, în vederea unor viitoare analize. Analiştii informaţiilor din cadrul fiecăreia dintre respectivele „staţii de ascultare" au liste separate de cuvinte, care îi ajută să analizeze conversaţii sau documente marcate de sistem, iar acestea sunt apoi transmise agenţiei de informaţii care a solicitat interceptarea. Se spune că Echelon este folosit şi pentru interceptarea supravegherii interne, a civililor americani, pe motive de afilieri politice „nepopulare" sau fără cauze evidente. Dacă e adevărat, atunci este vorba de spionaj politic şi sunt violate amendamentele 1, 4 şi 5 din Constituţia Americii.

Raportul Parlamentului European intitulat „O estimare a tehnologiilor de control politic", editat de Comitetul pentru Evaluarea Opţiunilor Ştiinţifice şi Tehnologice din cadrul Parlamentului European, ridică întrebarea dacă interceptarea comunicaţiilor de către Echelon nu violează suveranitatea altor state şi intimitatea cetăţenilor acestora. Nu prea mai există îndoială că staţia de la Menwith Hill îi supraveghează pe cetăţenii britanici pe teritoriul ţării, cu ştiinţa şi cu întreaga colaborare a guvernului britanic.

Echelon a fost creat cu sprijin de la GCHQ din Cheltenham şi, în 1993, elemente nemulţumite din interiorul comunităţii spionilor britanici au utilizat reţeaua pentru scurgerea unor informaţii privind încercările americane de a câştiga voturi la Naţiunile Unite în favoarea intervenţiei în Irak. Comunitatea britanică de spionaj a fost foarte nemulţumită de tentativele guvernului de a deforma informaţiile primite susţinând că Irakul menţinuse contacte cu reţeaua teroristă Al Qaeda. O femeie de 28 de ani, angajată a GCHQ, a fost arestată fiind suspectată de a fi încălcat Legea secretelor de stat. Se credea despre ea că ar fi lăsat să se scurgă un memoriu al NSA în care se solicitau informaţii din „liniile de produse“ (în jargonul SIGINT, asta înseamnă interceptări ale convorbirilor telefonice şi e-mailurilor), ordonând un „val“ de spionaj îndreptat împotriva ţărilor Angola, Camerun, Chile, Bulgaria şi Guineea, cu „un accent suplimentar pe problemele Naţiunilor Unite legate de Pakistan“. Scris de Frank Coza, şeful personalului de apărare (pentru obiective regionale), memoriul a fost pus în circulaţie, în acelaşi timp, de NSA. Operaţiunea, autorizată probabil de Condoleezza Rice, consultant pe probleme de securitate naţională, i-ar fi implicat, se pare, şi pe Donald Rumsfeld şi George Tenet, directorul CIA. Preşedintele Bush a ştiut cu siguranţă de ea. Scurgerea de informaţii a fost un act de sfidare atent plănuit, care a ilustrat nemulţumirea din serviciile secrete privind modul în care britanicii şi americanii întrebuinţau abuziv spionajul. Ruptura cu „seniorii“ din lumea informaţiilor se accentuase de ceva timp şi nu fusese ameliorată de dezvăluirea că în biroul lui Kofi Annan, secretarul general al ONU, fuseseră plantate microfoane de către americani.

Orice s-ar întâmpla, baza de la Menwith Hill continuă să crească şi aproape a dus la bun sfârşit proiectul Sistemului Infraroşu Spaţial (SBIRS), pentru care până şi NSA a fost obligată să ceară permisiunea Consiliului Districtual Harrogate înainte

de a-l putea instala. Nu există rachete sau alte sisteme aeriene de apărare în această bază, deşi nimeni nu se îndoieşte că, în eventualitatea puţin probabilă a unui atac nuclear, ea va fi una dintre ţintele principale. SBIRS este doar un alt nume pentru „Războiul Stelelor". Patru sateliţi noi au fost lansaţi pe orbită pentru a înlocui cele patru vehicule spaţiale excedentare din cadrul Programului de Sprijin al Apărării. Printre alte progrese, noul sistem poate detecta în spaţiu „corpuri reci", precum şi semnături cu infraroşii de la arderile motoarelor de rachete. Într-un discurs ţinut în faţa Congresului, generalul american Howell M. Estes III, şeful Centralei Nord-americane pentru Apărarea Aerospaţială, a afirmat că sistemele SBIRS vor îmbunătăţi capacitatea americanilor de a „oferi rachete balistice mai precise ca lansare şi punct de impact forţelor aflate într-un teatru de operaţiuni militare". Cu alte cuvinte, acurateţea şi ferocitatea puterii de foc americane, care sunt controlate din spaţiu, devin tot mai eficiente pe zi ce trece.

Frica şi furia induse de secretomania ce înconjoară Menwith Hill au creat, după cum era de aşteptat, şi revoltă politică. Speculaţiile privind activităţile desfăşurate de americani pe teritoriul britanic sunt nesfârşite. Europarlamentarii cer în mod regulat să afle exact ceea ce se petrece în baza militară, dacă americanii au primit acces la secrete ale comerţului european (ceea ce, evident, s-a întâmplat) şi dacă acest lucru periclitează securitatea europeană. Fără îndoială, e greu de imaginat că americanii ar tolera o unitate britanică sau europeană similară pe teritoriul lor, şi la fel de greu e de înţeles de ce această bază NSA nu ar trebui să răspundă în faţa guvernului britanic.

Ostilitatea locală faţă de staţia de la Menwith Hill reprezintă mai mult decât o ridicare din umeri ca în Yorkshire şi un bombănit „asta nu-i treaba mea, băiete". Localnicii vor să ştie ce se întâmplă dincolo de gardul de sârmă ghimpată şi de ce o bază atât de uriaşă nu primeşte forţă de muncă indigenă. Puţinii

tehnicieni şi analişti din Cheltenham care staţionează acolo reprezintă totalul implicării britanice. Scena din afara bazei aduce aminte de protestele antirăzboinice de la Greenham Common. O prezenţă constantă este cea a doamnelor trecute prin multe de la sediul local din Yorkshire al Campaniei pentru Dezarmare Nucleară (CND), care stau în corturi şi fac ceai la focuri aprinse cu surcele, provenind din foste barăci. Ele stau aici deja de ani buni şi acceptă cu seninătate că mai au destul de aşteptat. Protestatarii încalcă în mod obişnuit proprietatea, pătrunzând în bază, iar activităţile lor scot în evidenţă lipsa generală de umor sau de înţelegere a Armatei americane când vine vorba de asemenea demonstraţii. Rezultatul e că, din când în când, se întâmplă ceva care dovedeşte că până şi o unitate destinată războiului poate avea o parte ridicolă.

Atunci când, în 1997, două femei, Helen John şi Anne Lee, au făcut apel la condamnarea pentru violarea unei proprietăţi la Curtea Regală York, un avocat al British Telecom (BT) a fost chemat ca martor. Acest reprezentant al companiei a lăsat să-i scape informaţia că BT instalase trei cabluri din fibră optică cu capacitatea de a purta mai mult de 100 000 de apeluri telefonice simultan către baza militară americană. Avocatul, pesemne prost instruit de clientul său, a oferit Curţii de Apel detalii despre cabluri, pentru a fi apoi sfătuit de judecător să-şi retragă mărturia. Vechea „Poştă Generală“ (predecesorul BT) furnizase iniţial două circuite cu „lăţime de bandă mare“, pentru capacităţi ridicate, către Menwith Hill în 1975. Acestea erau conectate prin cablu coaxial cu reţeaua BT din Hunters Stones, o staţie radio cu frecvenţă înaltă, aflată aproape de baza americană. În anii 1970 şi 1980, aproape toate apelurile telefonice la distanţe mari treceau prin Hunters Stones. BT admitea acum că aceste cabluri erau conectate direct, suboceanic, cu Statele Unite. Cum a afirmat compania în mărturie, capacitatea de transmisie a fost triplată între timp, adăugându-se alte două legături prin fibră optică.

Avocatul BT a mai afirmat că alte companii de telecomunicaţii britanice au furnizat echipamente de interceptare bazei americane şi că aceste companii britanice erau implicate în activităţile de spionaj de la Menwith Hill. Revelaţiile datorate avocatului BT au fost întrerupte brusc de intervenţia judecătorului, care a acuzat martorul că divulgă secrete naţionale. BT a trimis apoi un al doilea avocat, în încercarea de a interzice mărturia. Astfel, recursul s-a transformat într-o farsă, însă un colţ al cortinei ce acoperă activităţile de supraveghere britanice a fost ridicat, chiar şi pentru scurt timp, pentru a dezvălui că guvernul nostru oferă americanilor nu doar informaţii militare, ci şi secrete comerciale, prin intermediul unor firme locale. Zi de zi, date furnizate de companii britanice devin disponibile analiştilor de la Menwith Hill.

Sediul Comunicaţiilor Guvernamentale (GCHQ), staţia de recepţie a guvernului din Cheltenham, este descris ca un „luptător împotriva infracţionalităţii" de către Comitetul Reunit de Informaţii, responsabil pentru el. De fapt, această bază este unul dintre cei mai sofisticaţi colectori de informaţii din lume. În 2004, el a fost mutat la periferia Cheltenhamului, unde fusese special construită o staţie de recepţie în care s-a investit un miliard de lire sterline. Securitatea informaţiei transmise din GCHQ se află în sarcina Grupului de Securitate a Comunicaţiilor Electronice (CESG). De intercepţia SIGINT se ocupă Organizaţia pentru Semnale Complexe, care are birouri în Cheltenham, dar şi în Cornwall şi pe insula Ascension.

GCHQ furnizează informaţii tuturor serviciilor de securitate şi le împarte cu baza de la Menwith Hill şi cu NSA. De fapt, organizaţia are personal comun cu americanii şi utilizează aceleaşi metode pentru a „semnaliza" informaţii de la sateliţi sau din alte surse electronice în şi din Insulele Britanice. GCHQ participă la sistemul american Echelon folosind dicţionarul Echelon pentru a captura „produse" – informaţii de spionaj

utile. O bună parte din activitatea GCHQ este limitată la agenţiile de informaţii britanice, însă organizaţia a fost implicată puternic în pregătirea Războiului din Irak, ceea ce a provocat supărarea multora dintre cei 3 500 de angajaţi de la Cheltenham – de aici, nemulţumirea şi scurgerile de informaţii.

Această formă de colectare a informaţiilor este menită să fie camuflată complet – există prezumţia că subiectul „trasului cu urechea" electronic nu este conştient că e spionat; altfel, informaţiile acumulate devin inutile. Însă există o modalitate mai directă – şi mai nepăsătoare – de a extrage informaţii de la suspecţii de terorism: tortura. Desigur, tortura este ilegală pe teritoriile americane şi britanice. Însă, atunci când eşti o organizaţie ce strânge informaţii care beneficiază de întregul sprijin al celor mai sus-puşi oameni ai ţării, se găseşte de obicei o cale de a ocoli o problemă minoră precum ilegalitatea. CIA şi NSA, disperate după o analiză a ameninţării teroriste, au extras liste de informaţii obţinute de la afgani şi alţi suspecţi din Orientul Mijlociu. Administraţia cerea rezultate şi le dorea rapid. CIA a intensificat folosirea a ceea ce e cunoscut drept „Transfer". Acest termen este o creaţie americană deosebit de cinică, susţinută fără ruşine de britanici. Ceea ce ne interesează aici este „Transferul extraordinar", un eufemism pentru „a te baza pe altcineva pentru a-ţi face treburile murdare".

Această practică, descrisă în termeni reci şi detaşaţi, sună ca o povestire scrisă de Franz Kafka în barul unui hotel, chiar înainte de ora închiderii. Ceea ce o face în mod special alarmantă este faptul că guvernul britanic cooperează entuziast, în deplină cunoştinţă de cauză, la ducerea la îndeplinire a acestei practici. Oficialii americani admit că „Transferul extraordinar" a fost folosit de CIA de cel puţin 200 de ori, ceea ce înseamnă aproape sigur că a fost folosit de mult mai multe ori, dar că această cifră este singura pe care îşi permit s-o recunoască. Se ştie că, în întreaga lume, diferiţi indivizi au fost răpiţi, hainele lor au fost

tăiate cu cuţitele, trupurile – umplute cu sedative, încheieturile mâinilor şi picioarele – înlănţuite, feţele – mascate şi acoperite cu glugi, corpurile – înfăşurate în scutece şi îmbrăcate în veşminte portocalii. Precum pachetele de carne, ei au fost transportaţi în avioane administrative Gulfstream către state precum Egipt, Maroc şi Uzbekistan, unde extragerea de informaţii prin metode precum fierberea braţelor, ameninţarea cu aruncarea de pe o scândură în apă, lovirea repetată cu ciocane sau ataşarea unor electrozi de organele genitale sunt întâmplări cotidiene. Altfel spus, „Transferul extraordinar" este pur şi simplu un eufemism pentru forţarea suspecţilor de a-şi mărturisi implicarea în acte teroriste, prin supunerea lor la torturi. Singurul motiv imaginabil pentru care americanii sunt gata să facă asta este credinţa lor că scopul scuză mijloacele. Ei sunt convinşi că acei oameni sunt terorişti militanţi şi că, din moment ce organizaţiile de impunere a legii sunt restricţionate de reguli procedurale stricte în ţările lor, ei nu dispun de mijloacele legale de a-şi supune suspecţii nivelului de presiune fizică şi emoţională necesar pentru a-i forţa rapid să vorbească.

Calitatea informaţiilor obţinute prin tortură fizică şi mentală este recunoscută ca inferioară. Am discutat despre asta cu un ofiţer din Divizia Specială, cu o experienţă îndelungată în interogarea suspecţilor IRA; el a comentat: „Poţi convinge pe cineva să spună orice, dându-i speranţa că vei înceta să-i mai provoci durere. Asta nu înseamnă că spune adevărul". Şi a continuat: „Există metode mai rapide şi mult mai eficiente de a obţine acelaşi lucru. Tortura pur şi simplu nu funcţionează ca mijloc de obţinere a unor informaţii semnificative". Motivaţia care îi determină pe americani să recurgă la asemenea acţiuni sălbatice şi nejustificate este dublă. În primul rând, procesul legal în Statele Unite este interminabil şi scrupulos, cu procese de apel întinse şi referiri constante la drepturile omului. Sistemul penal american este recunoscut drept brutal, însă numai pentru aceia

condamnaţi pentru infracţiuni. Golful Guantánamo din Cuba găzduieşte suspecţi fără reprezentanţi legali, care pot fi trataţi ca neavând drepturi cetăţeneşti. Atât cât este implicată administraţia Bush, teroriştii nu sunt protejaţi de Convenţia de la Geneva, dar, pentru a evita stânjeneala, suspecţii sunt ţinuţi departe de patrie şi de orice posibilitate de obstacol legislativ, fiind întemniţaţi în unităţi secrete, controlate de CIA, din întreaga lume. Agenţiile de securitate americane implicate sunt judecate după rezultate, iar o mărturisire, chiar şi sub constrângere, echivalează cu un bonus. De asemenea, teama de a fi capturat şi transferat în secret într-o celulă subterană, în barăcile secrete din Cairo, îl va preocupa chiar şi pe cel mai înfocat „luptător pentru libertate“, iar zvonurile despre ororile care aşteaptă pe oricine e suspectat de CIA s-au răspândit rapid în întreaga lume arabă.

În 2005, George W. Bush a fost întrebat, la o conferinţă de presă de la Casa Albă, despre practica „Transfer extraordinar“, la care recurg agenţii CIA. Preşedintele a ezitat să răspundă, a examinat podeaua, a făcut o pauză, şi-a aruncat privirea prin încăpere, a tuşit, apoi a şoptit că practica există, dar este justificată, deoarece „este o măsură antiteroristă şi nu există nimic ce nu aş face pentru a împiedica moartea cetăţenilor americani“. Cu două luni mai devreme, pe 27 ianuarie, într-un interviu pentru *New York Times,* Bush declarase: „Tortura nu este niciodată acceptabilă. Noi nu trimitem niciodată oameni în ţări care practică tortura“. Aceasta a fost o minciună sfruntată.

Există, din păcate, prea multe dovezi privind practicarea „Transferului extraordinar“ pentru a ne mai îndoi că această practică are loc. Mai rău e că, prin recurgerea la asemenea metode extreme, Statele Unite îşi trag la fund şi prietenii, şi aliaţii. Avioanele utilizate şi operate de CIA, sub numele de cod „Transport administrativ prioritar“, îşi fac plinul în mod regulat în baze ale Forţelor Aeriene Regale şi în aeroporturi civile din Marea Britanie, iar informaţiile obţinute prin tortură ajung

la analiştii de spionaj britanici, care le examinează cu sânge rece. Principala problemă pe care o au de înfruntat echipajele de navigaţie şi asasinii cunoscuţi ca „Unitatea Specială de Evacuare“, care efectuează aceste transferuri în timpul programului lor de zbor în jurul lumii, a fost, dintre toate, marele amator de aviaţie britanic. Această pasiune puţin cam aiurită s-a transformat într-o reţea de membri largă şi foarte eficientă. Un avion Gulfstream cu numărul de înregistrare N379P a fost asociat de ei cu o firmă de chartere numită „Premier Executive Travel“, o companie-fantomă cu sediul în biroul unor avocaţi de la periferia Massachusettsului şi un preşedinte cu o adresă înregistrată în Arlington, Virginia, aproape de sediul CIA. Avionul a fost observat în mod regulat făcând curse în spaţiul aerian britanic; se ştie că a aterizat la Brize Norton, Mildenhall, RAF Leuchars, Luton şi Glasgow. Intrările în şi ieşirile din Marea Britanie i-au fost notate cu mare sârguinţă de către detectorii de avioane şi înregistrate în bazele lor de date, potrivit lui Chris Yeats, un expert în operaţiuni aeriene. Avionul a fost prezent de atâtea ori aici fie pentru a-şi face plinul, fie pentru a lua parte la procesul de „Transfer“ din Marea Britanie către medii mai puţin blânde din Africa şi Orientul Mijlociu. Agenţiile de spionaj americane utilizează în mod obişnuit avioane ale unor companii particulare pentru operaţiile lor, cu scopul de a distrage atenţia de care au parte în general avioanele militare. Oricum, CIA a greşit neluându-i în calcul pe pasionaţii de aviaţie britanici.

Odată ce ziariştii au descoperit că o companie de aviaţie privată sprijinea CIA şi au început să pună întrebări incomode, sediul firmei Premier Executive Travel şi detaliile sale de înregistrare au fost imediat modificate. Se ştie că avioane particulare având la bord agenţi CIA au aterizat şi pe aerodromul Broma din Suedia, unde forţele speciale de intervenţie au ridicat doi egipteni de pe o stradă lăturalnică din Stockholm. Cei doi erau suspectaţi de asocieri cu Al Qaeda şi au fost ţinuţi în Suedia

timp de opt ore, înainte de a fi sedați și transportați cu avionul la Cairo, unde au fost închiși și supuși timp de câteva luni la torturi și interogatorii. Unul din ei, doctorul Aziza, a reușit să dea un telefon soției sale Hanna înainte de a fi drogat de Unitatea Specială de Evacuare. Doctorul Susan Fayed, lucrător medical la Nadim, un refugiu solitar egiptean și un centru de reabilitare pentru victime ale torturii, mi-a spus că primesc persoane care au fost ținute în închisoare și eliberate cu fracturi, arsuri și paralizie provocate de tortura cu electricitate. Ea afirmă că doctorul Aziza a fost vizitat de mama sa, după ce torturile începuseră să își facă efectul, și se afla în stare șocantă. Ulterior, el a fost condamnat la 25 de ani de muncă silnică. Tovarășul său a fost eliberat și este arestat la domiciliu în Cairo; e prea îngrozit pentru a vorbi despre experiențele sale. „Americanii știu ce se petrece acolo, spune doctorul Fayed. Multe dintre victimele pe care le-am văzut la centrul Nadim au fost aduse aici de Unitatea Specială de Evacuare."

Craig Murray, ambasadorul Marii Britanii în Uzbekistan (o mică și urâtă dictatură, înghesuită între Afganistan și Rusia), a realizat că este urmărit atunci când a fost invitat la cină de profesorul Jamal Mirsaidov, un militant pentru drepturile omului din Tașkent. A doua zi, nepotul lui Mirsaidov a fost găsit torturat până la moarte. Fusese bătut cu bare de fier și apoi fiert de viu. Autoritățile uzbece au pretins că de fapt căzuse victimă unei supradoze. Murray a devenit îngrijorat atunci când a descoperit, dintr-o conversație cu un agent MI6, că serviciile de securitate britanice considerau că informațiile transmise din Uzbekistan către CIA și MI6 erau de cea mai înaltă calitate și încredere. El a revenit la Londra în 2003, pentru a protesta în fața superiorilor săi din Ministerul de Externe, care primiseră consultanță legală de la unul dintre magistrații lor, un anume M.C. Wood. Acesta a confirmat că este legal „să deții informații obținute prin tortură". Murray a discutat cu Jack Straw,

ministrul de externe, care i-a declarat că, deşi are „nopţi nedormite din cauza asta", trebuie să urmeze sfatul serviciilor de spionaj.

Lăsând deoparte implicaţiile morale ale actualei forme de colectare a informaţiilor, în care totul este permis, consider că serviciile de securitate americane şi britanice sunt vulnerabile la farse şi greşeli, cum se întâmplă peste tot. Acest lucru este valabil mai ales în cazul supravegherii. „Spionilor" le place să spună că doar eşecurile şi erorile se află, pentru că restul e secret. Aşa o fi, dar cum putem noi şti asta? Un exemplu faimos: americanii n-au reuşit să prevadă atacurile Al Qaeda asupra World Trade Center, în pofida faptului că Osama Bin Laden mai încercase o dată să distrugă clădirea, punând un om al său să planteze un camion-bombă în subsolul ei. De fapt, eşecurile spionilor americani şi britanici au o istorie mult mai lungă. Serviciile secrete americane nu au ratat doar Pearl Harbor, ci şi căderea Zidului Berlinului, şi n-au avut habar de decizia lui Hruşciov de a trimite rachete în Cuba până când armele nu au fost fotografiate *en route* de un avion-spion U2. Spionii britanici nu au reuşit să prevadă închiderea Canalului de Suez de către preşedintele Egiptului, Gamal Abdel Nasser, care a generat o criză în 1956. Ei au fost prinşi nepregătiţi de începerea campaniei cu bombe a IRA, de căderea şahului Iranului sau de invadarea insulelor Falkland de către Argentina. Când e vorba de aflarea unor detalii precum locul unde îşi ascunde Mugabe milioanele strânse din jafuri sau sub ce acoperiş îşi cultivă marfa un traficant de droguri, avem cu siguranţă cunoştinţele şi capacitatea de a afla adevărul. Mai ştim şi multe lucruri privind obiceiurile şi slăbiciunile subiecţilor noştri, deoarece – cum am văzut deja – suntem de departe cea mai supravegheată ţară din lume. Însă, atunci când vine vorba despre predicţiile amănunţite şi analiza marilor evenimente, se pare că nu dispunem de competenţa de a cerne informaţiile, de a le examina

amănunţit şi de a pune planuri la cale, iar americanii stau la fel de prost ca noi.

Incapacitatea de a prevedea marile evenimente, în ciuda informaţiilor deţinute de agenţiile ce operează în numele statului, se datorează cu precădere incapacităţii de a analiza ce s-a aflat până acum prin spionaj, mai ales din pricina calităţii personalului angajat de serviciile de securitate şi a „factorului uman", supus greşelii. Toate marile puteri sunt mai preocupate să acumuleze informaţii decât să le analizeze. Lipsa unei unităţi, a unei clarităţi a scopului şi a unei viziuni de ansamblu a diverselor agenţii de informaţii creează erori politice deseori catastrofale, care ies la iveală după evenimente. Misiunea oficială a CIA este aceea de a furniza informaţii externe exacte, bazate pe dovezi, cuprinzătoare şi de actualitate privind securitatea naţională, precum şi de a desfăşura activităţi de contraspionaj, activităţi speciale şi alte funcţii asociate cu informaţiile externe şi securitatea naţională, la ordinul preşedintelui. Dacă obiectivul este ca informaţiile să fie bazate pe probe, cine stabileşte parametrii? Şi de ce nivel al dovezilor este nevoie pentru a justifica „activităţile speciale"? Desigur, se prea poate ca această declaraţie să fi fost redactată de un omuleţ în pantaloni de bumbac bej, locuind pe Madison Avenue, căruia sintagma „activităţi speciale" i-a atras atenţia şi i-a provocat un fior. Nu se ştie niciodată.

În schimb, ştim că bugetul anual al comunităţii agenţiilor de informaţii din SUA este de 40 de miliarde de dolari, deşi se pare că încă le mai scapă subiectele mari. La fel ni se întâmplă şi nouă. Chestiunea rateurilor serviciilor secrete va fi abordată mai detaliat în capitolul IX.

CAPITOLUL VII

Ochiul din cer

Avem cu toţii o vagă idee despre nişte piese metalice sofisticate numite sateliţi, care orbitează deasupra capetelor noastre; credem că sunt, în general, un lucru bun. Ei nu sunt utilizaţi doar pentru a explora spaţiul cosmic, dar ne aduc televiziuni din întreaga lume şi sprijină sisteme de radionavigaţie prin satelit (GPS) sau resurse puternice pentru telefonia mobilă. Ei observă vremea şi pot urmări chiar şi evoluţia furtunilor de nisip din Africa de Nord. Sateliţii mai sunt folosiţi pentru a trasa mişcările globale ale peştilor şi animalelor; de exemplu, chinezii utilizează supravegherea prin satelit ca să monitorizeze obiceiurile de migraţie ale populaţiei sale de 4 000 de cocori cu gâtul negru. Uniunea Europeană verifică dacă terenurile nelucrate pentru care fermierii primesc beneficii nu sunt cultivate, iar extinderea incendiilor forestiere este urmărită pe întreg globul, de la arhipelagul grecesc până la Amazon.

Supravegherea prin satelit a fost foarte eficientă în stăvilirea poluării cu petrol cauzate de practica – foarte răspândită odinioară – a navelor comerciale de a-şi goli rezervoarele de petrol în larg. În 2005, se aflau pe orbită 31 de sateliţi, ce ofereau imagini ale suprafeţei terestre, cu rezoluţii similare fotografiilor făcute de la 1 la 30 de metri. Dintre aceşti sateliţi, 14 sunt finanţaţi privat de corporaţii americane, fiecare dintre

ei având imagini cu rezoluții corespunzătoare la cel mult zece metri. Sistemele ieftine de sateliți comerciali, care devin operaționale în prezent, oferă imagini cu rezoluții chiar și mai bune, iar ei vor deveni o parte importantă a marketingului orientat către consumatori, fiind utilizate pentru a monitoriza traseul mărfurilor pe întreg globul. Însă nu este oare deranjant să ne gândim la „atotștiutorul ochi din cer“, care poate alege din mulțime pe oricine dintre noi și să-l urmărească pretutindeni, atât cât are el chef? Cum ne putem proteja intimitatea de asemenea sisteme îndepărtate, dar foarte eficiente, care operează într-un spațiu ce nu se supune normelor legii sau votului democratic? Țări din întreaga lume – și mai ales Statele Unite – cheltuiesc sume imense pentru a face cât mai mici tehnologiile ce le permit să-și bage nasul peste tot. Drept rezultat, camera-spion nu trebuie să fie pe orbită, în spațiu, pentru a vedea ce faci; ea poate pluti într-un colț al încăperii tale.

Dintre toate sistemele de spionaj, ce mă supără cel mai mult este gândul că pot fi urmărit de sateliți. Nu e suficient de rău că sunt camere de supraveghere pe străzi și în magazine, că trebuie să completez formulare intruzive pentru agenții guvernamentale precum Administrația Financiară și să-mi dovedesc identitatea de fiecare dată când ajung, în concediu, pe aeroportul Kennedy, acum mai trebuie să fiu conștient și de un fapt menit să-mi distrugă nervii: un lucru invizibil din spațiu este capabil să mă identifice sau să-i identifice pe prietenii mei, precum și să înregistreze tot ceea ce facem. Chiar și mai mult mă îngrijorează o întrebare: dacă poate fi amplasat echipament în spațiu care să ne monitorizeze fiecare mișcare cotidiană, fără ca noi să putem spune ceva în această privință, ce altceva pot ei lansa pe orbită, deasupra capetelor noastre, și ce va face acel lucru? Progresul științific adus de cursa pentru cucerirea spațiului și de inițiativa „Războiul Stelelor“ a lui Ronald Reagan a scăpat de sub control, iar acum în Statele Unite se vorbește despre războaie purtate în spațiu.

Cel mai puternic mijloc de a-şi spiona inamicii şi cetăţenii de care dispune America este satelitul „Keyhole“ (KH – „gaura cheii“). Fiecare costă 1 miliard de dolari şi, totuşi, tot ceea ce se ştie deocamdată despre mişcările sale în spaţiu este că operează la diferite altitudini de alţi sateliţi – detaliile orbitelor lor de deasupra Pământului sunt strict secrete. Numărul exact de sateliţi KH activi este de asemenea necunoscut, deşi în general se acceptă că există vreo 200 pe orbite „fixe“ (adică se mişcă cu aceeaşi viteză ca şi Terra, aşa că rămân în aceeaşi poziţie în raport cu planeta de sub ei) şi că grămezi dense sunt poziţionate deasupra unor locuri cu probleme, precum Orientul Mijlociu şi Coreea de Nord.

Sateliţii artificiali sunt creaţi pentru a îndeplini funcţii specifice. Un satelit de comunicaţii, de pildă, îmbracă de obicei forma unei farfurii sau umbrele, cu antene multiple. Flota KH este cheia succesului lui Echelon, cel mai mare sistem colector de informaţii din toate timpurile, şi, de asemenea, a dezvoltării şi a utilizării de arme în spaţiu. Sateliţii KH sunt lansaţi pe orbită de pe navete spaţiale NASA sau de pe rachete Titan. În esenţă, ei sunt camere digitale orbitale, echipate cu lentile foarte puternice, capabile să detecteze obiecte de pe sol care nu au mai mult de 12 centimetri de-a curmezişul. Asta înseamnă că pot citi plăcuţe de înmatriculare ale autovehiculelor sau titlurile dintr-un ziar, precum pot şi să identifice o bandă de încărcare a unei arme. Programul camerei de supraveghere scanează obiectul şi fie îl înregistrează imediat, fie, dacă vizibilitatea este proastă, ia o decizie automată de a produce o imagine de calitate mai bună. Imaginile transmise de sateliţi sunt analizate la Agenţia Naţională de Imagistică şi Cartografiere, care oferă agenţiilor de securitate guvernamentale, la cerere, datele obţinute.

În teorie, informaţiile adunate de sateliţii KH pot fi folosite pentru colectarea de date din spionajul militar sau pentru cercetarea ştiinţifică. Totuşi, NSA şi CIA beneficiază şi ele de aceste

informații, deoarece se știe, din dovezile aduse în tribunalele americane, că polițiile au folosit sateliții pentru a-i spiona pe cetățenii americani considerați „potențiali teroriști, persoane care pot încălca legea sau crea probleme“. Altfel spus, practic oricine poate fi vizat ca subiect al observației de flota sateliților ce orbitează Pământul.

Cunoștințele științifice necesare pentru a trimite senzori și pentru a lansa echipamente de filmare sofisticate pe o orbită stabilă deasupra planetei s-au dezvoltat rapid din primele zile ale cuceririi spațiului, iar sistemele de „ridicare“ care plasează sateliții în spațiu operează acum din întreaga lume. Unele mașinării spațiale sunt capabile să îndeplinească misiuni sofisticate și, ocazional, agresive. Este poate de înțeles faptul că atât de mult efort și resurse sunt utilizate în știința tehnologiei sateliților, având în vedere impactul pe care primul satelit artificial, Sputnikul sovietic din 1957, l-a avut asupra moralului națiunii americane când a fost lansat. Pe atunci, el a provocat mare îngrijorare, vecină cu panica, în Statele Unite. Chiar dacă Sputnik nu făcea în mare decât să transmită „bipuri“ printr-un radio ieftin ce plutea deasupra capetelor lor, americanii au simțit că spațiul lor aerian era violat, ceea ce i-a făcut să se simtă foarte vulnerabili. Tehnologia este astăzi mult mai rafinată. De la înălțimi de peste opt kilometri, satelitul de spionaj modern poate urmări și înregistra toate activitățile noastre cotidiene. El are senzori de căldură și tehnologii de obținere a unor imagini cu rezoluție mai bună, care îi permit să ne supravegheze în continuare, oriunde ne-am afla. Nu contează dacă o țintă umană se plimbă pe stradă sau conduce cu viteză pe autostradă sau se află în interior (într-o pivniță sau în ungherele ascunse ale unei fortărețe). Nici vremea nu schimbă cu ceva lucrurile. Subiectul poate la fel de bine să stea într-o închisoare sau în mijlocul unei furtuni cu trăsnete.

Deși pe orbită se află numeroși sateliți-spion, de fapt nu e nevoie decât de trei astfel de sateliți de ultimă generație pentru

a „vedea" întreaga lume. Pe lângă faptul că au puterea de a captura şi retransmite către sol imagini în timp real, ce altceva mai pot face ei? Pot controla de pe orbită sisteme de supraveghere electronică terestre sau să ne intercepteze conversaţiile din spaţiu sau chiar să lanseze arme? Americanii s-au bazat foarte mult pe tehnologia sateliţilor în timpul războaielor purtate de ei în Afganistan şi Irak. Această tehnologie le-a permis să intercepteze cantităţi vaste de informaţii din comunicaţii, prin sistemul Echelon, şi să le retransmită către sediul CIA din Langley, Virginia, prin Sediul Comunicaţiilor Guvernamentale (GCHQ), Menwith Hill şi multe alte staţii.

Desigur, americanii nu sunt singura naţiune ai cărei sateliţi de supraveghere orbitează Pământul. Spaţiul forfoteşte de aparaturi ocupate să înregistreze şi să transmită sau care doar dau ocol planetei, precum nişte corăbii aeriene. În prezent există 3 000 de sateliţi artificiali care operează pe orbită deasupra Pământului. Flota de sateliţi Astra, care transmite programe pentru B SKY B, are 12 sateliţi care orbitează la 35 880 de kilometri de Terra. Din cei 200 de sateliţi „Keyhole" americani lansaţi de la începutul anilor 1990, se crede că în jur de 150 funcţionează încă. Restul de 50 sunt excedentari şi s-au alăturat celor 6 000 de bucăţi de deşeuri spaţiale care orbitează planeta.

Graţie disponibilităţii largi de imagini de rezoluţie mare prin satelit, provenind din surse civile nerestricţionate, chiar şi naţiunile mai puţin prospere pot obţine acces instantaneu la supravegherea prin satelit, dacă îşi permit să plătească pentru ea. Imagini de valoare militară evidentă pot fi achiziţionate acum de efectiv orice ţară. De fapt, deşi puţine naţiuni îşi permit să conducă propriile programe de spionaj prin satelit, IKONOS, Quickbird şi alte sisteme private sunt accesibile în fond oricărei ţări, iar calitatea serviciilor oferite de ele este la un standard suficient de ridicat pentru a fi folosite chiar de CIA şi NSA.

Echipamentele de spionaj şi militare furnizează cele mai multe date „SIGINT" (semnale de spionaj) şi fotografice devorate de agenţiile de spionaj şi de forţele de poliţie din Marea Britanie şi America. Dacă vezi imaginile pe care ele sunt capabile să le transmită înapoi, îţi va fi aproape imposibil să accepţi distanţa de la care au fost luate. Departamentul guvernului american cel mai implicat în tehnologia de supraveghere prin satelit este Agenţia pentru Proiecte de Cercetare Avansată (ARPA), un braţ al Pentagonului. NASA se ocupă de sateliţii civili, dar nu există o linie strictă ce separă funcţiile civile şi militare. Administraţia Naţională pentru Aeronautică şi Spaţiu (NASA) lansează toţi sateliţii americani fie din Cape Kennedy (Florida), fie din baza forţelor aeriene Vandenberg (California) – indiferent dacă ei sunt operaţi de Armată, CIA, corporaţii sau lansaţi experimental de NASA ori pentru cercetarea spaţiului. E dificil de făcut o distincţie rapidă între sateliţii guvernamentali şi cei privaţi; cercetările realizate de NASA sunt deseori aplicabile tuturor tipurilor de echipamente de pe orbită. Nici ARPA, nici NASA nu se ocupă cu producţia de sateliţi; în schimb, ele garantează tehnologia, în timp ce diverse corporaţii furnizează echipamentele.

Armata americană îşi limitează deocamdată activitatea prin satelit la supraveghere, navigaţie şi comunicaţii. Dar pare sigur că forţele militare îşi vor extinde capacităţile până la a avea în viitor armament în spaţiu. Unul dintre motivele declarate pentru asta e faptul că există deja comerţ activ în spaţiu (sub forma sateliţilor de comunicaţii) şi acesta va avea nevoie să fie protejat. Oriunde ajunge comerţul american, acolo există şi interesul naţional şi necesitatea apărării lui. În 2002, Paul Teets, subsecretarul Forţelor Aeriene şi directorul Biroului Naţional de Recunoaştere, a declarat într-un discurs public că, în opinia sa, armele vor ajunge în spaţiu, iar asta „e doar o chestiune de timp". Teets ştie probabil ce zice, cu experienţa sa în dezvoltarea armelor de precizie, precum rachete şi bombe cu acurateţe

de 1 metru. Bombele ghidate prin laser şi rachetele ghidate prin GPS, precum Tomahawk, le-au dat deja forţelor militare o putere imensă, care poate garanta înfrângerea oricărui inamic cunoscut într-un război convenţional şi care, cu o tehnologie a sateliţilor corect desfăşurată, poate – cel puţin teoretic – să elimine victimele colaterale (civile). Trendul se îndreaptă către sisteme de armament mai precise şi letale, deseori controlate de la distanţă, capabile să răspundă comenzilor în câteva secunde şi să atace obiective de oriunde în lume, care au fost identificate de sateliţii „Keyhole". Pornind de aici, tehnologia spaţială şi utilizarea ghidării prin satelit vor oferi avantaje semnificative în viitoarele ostilităţi. Guvernul Statelor Unite, după experienţa sa de succes cu tehnologia spaţială în războiul purtat în Irak, studiază în mod activ următoarea generaţie de armament – armele laser şi „cinetice". (O să examinăm în curând ce pot face acestea.)

Potrivit ziarului *Washington Post,* preşedintele Statelor Unite şi comandanţii săi militari au acceptat că un anumit conflict în spaţiu este acum inevitabil şi se pregătesc pentru el. Abordarea reţinută a sistemelor de tip „Războiul Stelelor" din partea administraţiei Clinton a fost înlocuită de acceptarea fără rezerve de către administraţia Bush a exploatării inevitabile a spaţiului în scop militar. Este o perspectivă alarmantă. Tehnicienii nu doar studiază modalităţi prin care putem fi protejaţi din spaţiu, ci plănuiesc, de asemenea, folosirea tehnologiei spaţiale pentru a ne ucide.

Totuşi, costurile rămân marea problemă. „Ridicarea" sateliţilor este costisitoare în SUA. De aceea, furnizorii de sateliţi comerciali utilizează unităţile de lansare din ţări precum China, unde costurile sunt mai mici. Unul dintre cele mai importante astfel de locuri din afara Statelor Unite este Baikonur, din Kazahstan. Pentru a opera în mod tactic sateliţii, astfel încât ei să poată fi ridicaţi pe orbite mai depărtate, e nevoie de cantităţi enorme de energie. Noile generaţii de sisteme de înaltă putere

sunt de asemenea necesare pentru a activa şi întreţine arme ce folosesc lasere cu înaltă energie, evitând astfel reîncărcări frecvente şi costisitoare. S-a manifestat mult interes pentru tehnologii ce pot ajuta la micşorarea viitoarelor platforme spaţiale şi la reducerea cantităţii de energie necesară pentru lansare. Dispozitive micuţe, numite microsisteme electromecanice (MEMS), vor detecta căldura, lumina, mişcarea şi sunetul; ele pot fi utilizate într-o varietate de aplicaţii spaţiale, printre altele supravegherea şi controlul suprafeţelor reflectorizante din sisteme laser spaţiale.

Fiecare sistem de armament dezvoltat şi lansat va presupune un întreg „sistem de sisteme“, pentru a integra funcţiile de supraveghere, colectare, detectare şi evaluare a daunelor de război. Statele Unite prevăd pleiade de sateliţi, care vor fi mai puţin vulnerabili în faţa atacurilor, în timp ce acum, dacă un singur satelit ar fi atacat, asta ar putea scoate din circulaţie întreg sistemul. Câteva grupuri de sateliţi, gravitând la distanţe mici, ar putea oferi o acoperire globală „24 de ore pe zi, şapte zile pe săptămână“. Asta înseamnă că populaţia lumii ar putea fi sub o ameninţare constantă din partea unor arme aflate pe orbită, conectate cu sisteme de supraveghere.

Armele laser sunt pe cale să devină parte a arsenalului unei superputeri. Au fost deja concepute şi construite lasere chimice cu oxigen şi iodină, care pot fi utilizate şi ca arme. Laserele chimice sunt cercetate de când administraţia Reagan a propus sistemul de apărare împotriva rachetelor „Războiul Stelelor“, în anii 1980. În ultimii 20 de ani, aceste arme au cunoscut ameliorări semnificative în ceea ce priveşte sistemul optic, miniaturizarea, generarea de energie, controlul automat şi identificarea ţintei prin intermediul sateliţilor de supraveghere. Există tehnologia necesară pentru a produce un prototip care va permite atacarea ţintelor în câteva secunde sau minute – oriunde în lume. Forţele Aeriene Americane vor lansa acest tip de laser în sistemul

lor ABL (Airborne Laser System – Sistem Laser Aerian). Creat pentru apărarea de rachete balistice, el va fi în curând utilizat în mod regulat. Dezavantajele sistemului ABL sunt că trebuie aeropurtat pentru a fi eficient în timpul unui atac cu rachete balistice. Acest lucru face ca un sistem de arme laser aflate în spaţiu – şi în permanentă stare de aşteptare – să fie alegerea preferată de forţele armate. Un sistem de arme laser din spaţiu ar oferi o acoperire constantă, dacă ar fi utilizată o cantitate suficientă. Totuşi, armele laser nu sunt dintre cele care pot fi folosite pe orice vreme. Norii, ploaia şi efectele atmosferice pot disipa razele laser, impunând, astfel, creşterea puterii utilizate, pentru a le compensa. Totuşi, ele sunt arme flexibile, prin aceea că se poate controla cantitatea pagubelor produse, cu ajutorul duratei pulsului şi al puterii iradiaţiei. Materialele inflamabile vor lua foc la niveluri de iradiaţie destul de reduse, făcând mai ales din rafinăriile de petrol nişte ţinte vulnerabile. La niveluri de putere superioare şi cu o durată mai mare (care poate ajunge la câteva secunde), laserul poate să ardă şi să distrugă şi o ţintă mai solidă. Laserele de mare putere s-au dovedit eficiente deja în doborârea de rachete balistice, aflate în etapa de ascensiune, când sunt pline de combustibilul necesar învingerii gravitaţiei Pământului. De îndată ce se vor dezvolta în mod corespunzător şi generaţiile de lasere de mare putere, iar tehnicile de miniaturizare vor fi folosite pentru a se rezolva ridicarea instrumentelor pe orbită, armele laser spaţiale vor fi gata de a fi produse şi utilizate.

Americanii mai dezvoltă însă şi un al doilea sistem de arme spaţiale, care foloseşte tehnologia numită „cinetică". Armele cinetice sunt proiectile lansate de pe platforme din spaţiu şi ghidate prin GPS sau prin laser designator, o sursă de lumină laser utilizată pentru luminarea ţintei. Armele cinetice sunt extrem de precise, deoarece ele folosesc sisteme de ghidare similare cu cele utilizate de bombele şi rachetele cu ghidare de precizie – însă fără explozibili. Rachetele îşi obţin marele potenţial distructiv

prin viteza pe care o ating. Ajungând la o viteză hipersonică, ele pot produce forţe enorme, capabile să facă praf practic orice ţintă. Se spune că o armă cinetică poate distruge buncăre de comandă sau pline cu muniţie, aflate la sute de metri sub pământ. În funcţie de tipul de proiectile folosit, pot fi atacate ţinte singulare sau multiple.

Spre deosebire de lasere, armele cinetice vor putea fi folosite în orice condiţii atmosferice, putând fi lansate din sateliţi şi să lovească ţinte aflate oriunde pe pământ, în numai câteva minute. Aceasta le dă un avantaj imens faţă de lasere. Un alt avantaj este acela că armele cinetice nu necesită cantităţile imense de energie de care au nevoie armele laser. Ele vor opera în tandem cu sateliţii de supraveghere şi de ţintire „Keyhole“ şi vor fi lansate dintr-un grup de arme-sateliţi, lucru care le face, astfel, foarte dificil de atacat. Principala problemă a armelor cinetice o reprezintă căldura pe care o generează la reintrarea în atmosfera terestră, care poate deteriora serios receptorul GPS necesar pentru ghidare. Una din posibilele soluţii, testată la acest moment, ar implica folosirea unor lasere pentru a crea o undă-scut, care să protejeze proiectilul când trece prin atmosfera terestră. Este imposibil să te mai fereşti de o armă cinetică, odată ce aceasta a fost lansată. Singura măsură defensivă fezabilă împotriva unui atac cinetic ar fi folosirea unor arme antisatelit. Ele ar întrerupe sistemele de navigaţie prin GPS necesare pentru a ghida armele sau ar elimina satelitul înainte ca acesta să lanseze proiectilul. Tehnologia pentru a produce arme cinetice este deja disponibilă. Orice îmbunătăţiri ulterioare pe care le-ar suporta această tehnologie vor fi simple creşteri ale acurateţei sau ale potenţialului lor distructiv.

Ca factor determinant în influenţarea rezultatelor unui conflict şi prin aceea că duc la eliminarea totală a nevoii de arme convenţionale, ele nu vor altera, totuşi, balanţa puterii. Este foarte probabil ca, în cele din urmă, armele spaţiale să devină

un sistem de atac de precizie obişnuit, care mai degrabă sprijină celelalte sisteme de atac, în loc să le înlocuiască.

Războaiele conduse din spaţiu le vor permite comandanţilor – care, bineînţeles, se vor afla departe de câmpul de bătălie – să folosească sisteme de sateliţi fără echipaj, pentru a realiza supravegherea, identificarea ţintei şi distrugerea ei. Armele spaţiale vor avea cu adevărat o arie de cuprindere globală. Prima parte a programului, care este cel mai probabil să ajungă în spaţiu, este reţeaua de sateliţi de supraveghere necesari pentru identificarea ţintelor. Aceştia vor fi mai puternici decât orice a existat înaintea lor, capabili să vadă orice ungher ascuns de pe planetă.

Există motive întemeiate pentru îngrijorarea internaţională cu privire la posibilele distrugeri provocate de un război condus din spaţiu. Toate ţintele strategice vor fi vulnerabile în faţa atacurilor. Din pricina reacţiei rapide şi a vitezei armelor laser, tancurile, avioanele, vehiculele blindate, rachetele, elicopterele şi navele, aproape orice ţintă militară care are o suprafaţă poate fi ţintită şi distrusă. Navele aflate pe mare nu vor mai fi imune la atacuri, oriunde s-ar găsi. Acest tip de acoperire globală n-a mai existat până acum. Deşi bombardierele fixe B-2 pot acţiona cu precizie oriunde în lume, timpul necesar pentru ca ele să-şi atingă ţinta este mult mai lung decât cel necesar unei arme din spaţiu.

Este posibil ca armele spaţiale să joace un rol în acţiunile militare pe mare, dar prezenţa pe timp de pace şi misiunile de reacţie la criză, incluzând operaţiunile amfibii de contingenţă, nu vor dispărea niciodată. Marina militară va avea un rol viabil şi semnificativ de jucat. Portavioanele, ca piesă de rezistenţă a diplomaţiei naţionale şi centru al operaţiunilor de reacţie rapidă, vor continua să existe. Bineînţeles, ele vor deveni tot mai dificil de apărat şi, pe măsură ce tehnologia va evolua, va veni o vreme când nu vor mai avea unde să se ascundă. În cele din urmă, toate naţiunile vor trebui să joace un rol în controlarea

spațiului, pentru ca fiecare să-și poată apăra dreptul de a folosi spațiul maritim, aerian și terestru. De aceea, orice monopol al Statelor Unite în ceea ce privește desfășurarea de arme ofensive în spațiu ar fi temporar, în cel mai bun caz.

Evident, utilizarea de sisteme de sateliți ofensivi pe timp de pace va crea un imens scandal internațional. Toate națiunile care nu se consideră aliați ai Statelor Unite vor dori să dezvolte sisteme defensive. Supravegherea intruzivă de la bordul flotelor de sateliți „Keyhole" va fi prima țintă. În China, contramăsuri defensive sunt deja în lucru. Aceste măsuri sunt, fără îndoială, mai degrabă limitate pe moment, din cauza costurilor mari de dezvoltare și instalare pe care le presupun, dar este foarte probabil să se îmbunătățească în timp. În ultimul timp, au fost făcute multe încercări de blocare a sateliților de supraveghere americani. Controlul asupra logisticii spațiale, inclusiv logistica antisatelit, va avea în mod clar un impact asupra strategiilor și planificării militare viitoare. Statele Unite au rezistat în decursul istoriei plasării de sisteme de arme antisatelit în operațiuni, de aceea este de așteptat ca sistemele să rămână terestre. Dar, fie că vor avea baza în spațiu, fie că ea va fi terestră, misiunile de control spațial ale Statelor Unite vor trebui extinse. Utilizarea comercială a spațiului este extensivă, în special în domeniul comunicațiilor. Deschiderea spațiului către potențiale conflicte ar fi devastatoare pentru activitățile industriale și comerciale americane. Altfel spus, dacă Occidentului i s-ar refuza accesul la sateliții de comunicații comerciali, economia americană ar ajunge pe butuci într-un răstimp foarte scurt. Totuși, în general, asemenea viziuni futuriste nu se îndeplinesc așa cum se așteaptă. Armele spațiale pot fi un avantaj formidabil pentru comandații viitorului, însă un general va continua să se bazeze pe resursele convenționale. La fel cum armele nucleare nu au înlăturat cerința de capacități convenționale robuste, care includ flote și armate, este evident că armele ofensive cu

baza în spaţiu nu vor satisface toate nevoile militare – şi oricum, după cum am mai discutat, împotriva lor se dezvoltă deja contramăsuri.

Tehnologia informaţiei şi cantitatea imensă de date pe care, în acest moment, comandanţii din teren se bazează atât de mult, vin acum predominant cu ajutorul sateliţilor de comunicaţii. Chiar şi aşa, câteodată sunt insuficiente. Statele Unite investesc masiv în sisteme de rezervă, prin folosirea Vehiculelor Aeriene fără Echipaj (UAV-uri), care sunt capabile să ofere în timp real supraveghere, informaţii secrete şi informaţii despre ţinte. Sarcina lor este să devină o alternativă la sateliţi sau la acum demodatele avioane teleghidate „Predator“, care s-au dovedit atât de valoroase pentru supravegherea avansată în Războiul din Irak. Companiile britanice furnizează sisteme video şi GPS care sunt utilizate de oamenii de ştiinţă americani ce dezvoltă roboţi de supraveghere. University College din Londra a dezvoltat un vehicul de recunoaştere sub forma unui şarpe, conceput a se mişca pe pământ în maniera reptilei pe care o imită. El va fi lăsat la pământ dintr-un avion teleghidat şi va purta asupra sa instrumente capabile să transmită detaliile poziţiilor inamice. Computerul său se poate adapta, astfel încât să continue să transmită chiar şi după ce ar fi distrus. UAV-urile au fost dezvoltate pentru misiuni de recunoaştere în clădiri, tuneluri şi peşteri. Alimentate de ventilatoare contrarotante şi echipate cu aparatură sensibilă vizual, acustic şi în infraroşu, ele plutesc deasupra câmpurilor de luptă urbane şi transmit înapoi către liniile americane informaţii secrete.

O largă varietate de UAV-uri de toate tipurile (cum ar fi „Predator“) reprezintă acum o privelişte familiară deasupra Irakului. Ele sunt ieftine, discrete şi tind să fie folosite în special pentru adunarea de informaţii şi pentru supraveghere. Însă există o tendinţă către aparatură de dimensiuni mult mai mici. Încă din 1995 sunt în dezvoltare aparate de zbor microscopice. În

ultimii cinci ani, scopul a fost acela de a imita insectele zburătoare, atât în ceea ce priveşte zborul, cât şi mărimea. De exemplu, felul în care un fluture se mişcă în zbor este bine înţeles şi poate fi copiat de către oamenii de ştiinţă. Au fost construite prototipuri care zboară cu uşurinţă. Acum 20 de ani, companii americane precum Aeronvironment proiectau şi testau maşini de zbor minuscule, alimentate cu baterii pe litiu şi care erau încărcate cu echipament de zbor, computer, cameră video şi transmiţător. Modelele iniţiale, precum Văduva Neagră, care funcţiona cu ajutorul unei elice, avea 15 cm lungime şi cântărea 56 g. Era capabil să producă o imagine de mare precizie. Maşinile de zbor miniaturale moderne rămân secrete, deoarece sunt încă folosite, şi nu doar de către agenţiile secrete, ci şi de către companii private, cu scopuri ascunse. În mod clar, un derivat al cercetării militare, aplicat în sectorul privat, va fi abilitatea de utilizare a microroboticii ca mijloc de transport al unor sisteme de supraveghere sofisticate în medii serios protejate.

Acum câţiva ani, Biroul pentru Cercetări Navale al Statelor Unite a construit şi testat un prototip de aparat de zbor teleghidat pentru spionaj mai mic decât o monedă de un penny. Variantele recente sunt mai mici, mai puternice şi folosesc puterea solară pentru a acţiona patru aripi membranare, care se zbat cu 180 de bătăi pe secundă şi care le permit să creeze portanţă. Aripile poartă pe ele aşa-numitul „praf magic“ – cipuri microscopice de computer care reprezintă creierul vehiculului. În Statele Unite, au fost raportate insecte zburătoare manufacturate şi dezvoltate de Georgia Tech Research Institute – minuscule, telecomandate şi produse în masă –, care au fost folosite pentru a se infiltra în clădiri şi a rămâne nevăzute. Tehnica este numită „biomimetrică“, făcând referinţă mimarea sistemelor biologice şi adaptarea lor pentru cerinţele umane. „Insectele“ pot transmite date la mare distanţă. Unele dintre ele sunt folosite în sistemele de ghidare şi adaptate la proiectele rapide şi

ieftine de curăţare a minelor. Ele sunt proiectate să profite de condiţiile atmosferice proaste pentru a pătrunde cât mai adânc în teritoriile inamice. Au mai fost dezvoltate şi alte concepte, care folosesc motoare cu reacţie miniaturale, alimentate cu hidrocarburi şi capabile să zboare zeci de kilometri cu viteze de 80 km pe oră. RMB Miniature Bearings, o companie elveţiană, a produs motoare electrice care cântăresc o treime de gram. Iar oamenii de ştiinţă de la Massachussetts Institute of Technology au dezvoltat un motor cu reacţie care măsoară 10 mm pe 3 mm şi care este alimentat cu motorină sau benzină.

Bineînţeles, acestea sunt jucării pentru spioni – adevărata muncă murdară este dusă la îndeplinire de către cei care analizează datele culese, de aparatura de spargere a codurilor şi de computerele masive încuiate în camere aseptice, în peisaje rurale îndepărtate, peste tot în această lume. Ştiinţa roboticii miniaturale şi folosirea prafului magic au fost în stadiu de dezvoltare timp de mulţi ani, iar Pentagonul n-a dezvăluit stadiul cercetărilor. Nu există nici o îndoială că tehnicile la care au lucrat au produs dividende, atât în colectarea de informaţii secrete, cât şi în supravegherea câmpului de luptă. Problema este că aceste aparate vor trebui operate de către oameni, cărora politicienii le vor spune ce să facă. Şi probabil acesta este punctul din care lucrurile ar putea începe să meargă prost.

Tehnologiile militare şi cele comerciale se dezvoltă separat, însă sunt reunite regulat pentru aplicaţii reciproc benefice. Progresul uluitor al tehnologiei civile de supraveghere la distanţă aplicată la câmpurile moderne de luptă presupune că tehnologia de luptă a atins deja un stadiu de dezvoltare la limita SF-ului. Impulsul pentru ceea ce a ajuns să fie numită „tehnologia de luptă la distanţă“ a venit de la americani, care au prevăzut, într-o oarecare măsură, conflictele armate necomplicate de scrupulele morale care bântuie alte naţiuni. Spre deosebire de britanici, care au recurs la acuzarea propriilor soldaţi care au ucis irakieni

în timpul acțiunilor militare împotriva insurgenților, prioritatea americanilor a rămas siguranța forțelor lor armate și a propriilor cetățeni. Chiar și atunci când un soldat american a fost înregistrat pe cameră cum omoară cu sânge rece trei prizonieri răniți și neînarmați, acest lucru nu a dus la acuzarea lui. Statele Unite nu au aderat niciodată la Curtea Penală Internațională, iar dacă un soldat american spune că s-a simțit amenințat atunci când a deschis focul, este foarte puțin probabil ca el să fie acuzat vreodată. De fapt, nu au existat acuzații penale împotriva soldaților americani care au luat parte la bătălie, în timpul sau după Războiul din Irak. Această atitudine le permite să dezvolte tehnologii militare care ar putea să nu fie considerate acceptabile de către forțele armate britanice. Un exemplu ar fi introducerea roboților atât ca instrumente de supraveghere, cât și ca mașini de ucis.

Utilizarea de aeronave teleghidate drept vehicule lansatoare de rachete a devenit acum un lucru obișnuit. Programele de dezvoltare a tehnicilor robotice de război – Sistemul Direct de Acțiune pentru Observarea și Recunoașterea Armelor Speciale (SWORDS) – și armele pe care le-au dezvoltat au fost utilizate în situații de luptă din Afganistan și Irak. La începutul anului 2005, America a început să trimită roboți înarmați în Irak. Roboții aveau inițial un rol de recunoaștere în teritoriul inamic, dar și capacitatea de a executa foc mortal. Acești roboți ai începuturilor sunt de fapt vehicule monitorizate, telecomandate, care pot fi operate de la o distanță de o mie de metri de către un soldat echipat cu un laptop. Ei sunt înzestrați cu sisteme de navigare prin GPS, camere video și arme automate de foc rapid, iar unele variante pot fi înarmate chiar cu lansatoare de grenade și rachete antitanc.

O mașină poate ucide fără remușcări sau sentimente de vinovăție și poate fi și rapidă. Pentagonul a alocat 70 de miliarde de dolari roboticii militare, într-un program denumit „Sisteme de

Luptă ale Viitorului", iar cu acest gen de investiţii şi cu viteza rapidă a dezvoltării tehnologice, în curând roboţii vor fi folosiţi în mod curent. Totuşi, britanicii sunt preocupaţi de chestiuni etice şi de legalitatea acestor roboţi pe câmpul de luptă. În august 2004, un pilot al Forţelor Aeriene Regale (RAF), folosind un sistem computerizat, la o bază a Forţelor Aeriene ale SUA din deşertul Nevada, a putut controla un avion teleghidat de tip Predator, care zbura la 3 218 kilometri distanţă, deasupra Irakului, şi a lansat o rachetă Hellfire direct la ţintă – o fortificaţie a unui grup de insurgenţi.

Un fost şef din Comanda Strategică mi-a spus: „Ne antrenăm piloţii să evalueze şi să identifice ţintele înainte de a deschide focul. Pilotul RAF care opera avionul Predator de pe teritoriul Statelor Unite acţiona sub incidenţa legii britanice şi a unui regulament de angajare britanic. Dar suntem preocupaţi de eficienţa armelor telecomandate într-un câmp de luptă urban aglomerat. Putem noi să garantăm că un robot va putea să facă distincţia între un insurgent armat şi o femeie cu un copil mic în braţe? Cum poţi să programezi un robot să ia decizii de viaţă şi de moarte cu viteza fulgerului, în condiţii haotice de luptă? Un soldat trebuie să se bazeze pe instinct şi antrenament şi trebuie să ia decizii dificile instantaneu. Nu cred că ne putem aştepta încă la aşa ceva din partea unei maşini. Am fi îngrijoraţi de posibilitatea ca maşina să funcţioneze prost. Ştiinţa roboticii de luptă se află încă la începuturi şi se bazează pe tehnologii precum semnalele radio şi transmiterea de imagine, lucruri cu care se poate uşor interfera".

Schimbări revoluţionare în modul în care sunt conduse războaiele şi supravegherea în secolul următor nu pot fi prezise bazându-ne doar pe prezenţa armelor spaţiale ofensive, a roboticii şi a dezvoltării sistemelor de supraveghere miniaturale. În cele din urmă, războiul se reduce întotdeauna la un conflict uman – om contra om, esenţa bătăliei. Scopul ultim al cercetării

în domeniul roboticii este acela de a produce o mașină care să poată face tot ce poate face un soldat. Americanii estimează costul eventual al unui astfel de robot la aproximativ 10% din cel al contrapartidei sale umane. După Geoff Grossman de la Centrul de Cercetări al Forțelor Unite Americane, deocamdată, tehnologia poate oferi puterea de procesare computerizată echivalentă celei a unui mamifer.

Armele antisatelit vor avea un loc semnificativ în planificarea militară viitoare, care folosește tehnologia din bazele terestre sau spațiale. Nici o țară nu a admis efectiv că plănuiește sisteme de arme antisatelit, și în nici un caz în spațiu. Dar dezvoltarea armelor laser și a celor cinetice merge înainte și ar putea în curând să însemne folosirea de arme în spațiu, lucru care ar duce la încă o cursă a înarmării. Nu există răspunsuri ușoare. Pe moment, Statele Unite și Marea Britanie, cu tehnologia Echelon filtrată prin flota proprie de sateliți Keyhole, au obținut cea mai mare realizare a spionajului pe care a cunoscut-o vreodată lumea. Iar acum se discută despre cum vor fi înarmate sistemele de supraveghere.

Există multe întrebări la care politicienii și strategii militari americani trebuie să răspundă. De exemplu, vor putea Statele Unite să-și permită noi sisteme de arme spațiale? Se vor abține celelalte națiuni de la a contrabalansa eforturile americane în spațiu, odată ce Statele Unite vor încălcă moratoriul privind armele în spațiu? Iar aceste arme spațiale ofensive vor amenința oare stabilitatea lumii? Mulți vor argumenta că e timpul să se cadă de acord asupra interzicerii oricăror arme în spațiu. Tehnologia sateliților și tehnica de război bazată pe aceștia necesită un nou set de reguli de conduită de război și dezvoltarea de noi strategii de către armate.

Instalarea de arme spațiale ofensive pe orbită va fi o chestiune controversată, și nu doar în Statele Unite, ci oriunde în lume. Politicienii și oamenii de știință vor dezbate problema înainte ca

„Ultima Frontieră“ să devină un câmp de luptă. Este probabil ca publicul american să susţină armele spaţiale defensive, cum ar fi sistemele antisatelit, în special ca urmare a lui 9/11. Într-adevăr, mulţi americani par să creadă, având în vedere ce consideră ei a fi ameninţarea „terorii globale“, că dorinţa de intimitate este o chestiune futilă, că folosirea unor tehnologii de supraveghere prin satelit mai intruzive şi desfăşurarea de arme spaţiale sunt de la sine înţelese. Statele Unite ar putea deveni atunci prima naţiune care să încalce moratoriul internaţional cu privire la plasarea de arme ofensive în afara atmosferei Pământului. Înarmarea unilaterală a spaţiului ar reprezenta un dezastru pentru relaţiile dintre Statele Unite şi aliaţii lor de oriunde de pe glob. Deşi nu vor fi încălcate nişte tratate anume, orice urmă de încredere că Statele Unite ar fi dispuse să respecte aceleaşi reguli de conduită internaţională ca şi alte ţări ar dispărea pentru totdeauna. Marea temere a majorităţii ţărilor este aceea că, dacă militarizarea spaţiului ar începe din cauza unui electorat american dezinteresat, consecinţele potenţiale vor fi devastatoare – ar putea însemna distrugerea planetei. Ar fi corect să spunem, totuşi, că administraţia Bush nu a părut prea preocupată. Pare de neconceput că armele spaţiale ar putea vreodată să atingă puterea distructivă a celor nucleare. Desfăşurarea de arme nucleare în spaţiu ar marca, în mod potenţial, începutul sfârşitului rasei umane. Dar, deoarece „războiul spaţial“ se află încă în primele sale faze, armele nucleare ar putea fi privite pur şi simplu ca instrumente de descurajare. Fără îndoială că politicienii vor invoca scuza că armele nucleare din spaţiu nu vor fi folosite decât în circumstanţe excepţionale. Însă cine va decide care sunt aceste circumstanţe?

CAPITOLUL VIII

Lege şi dezordine

Forţele de poliţie britanice se confruntă cu o nouă lege penală la fiecare trei zile. Este, desigur, foarte greu să ţii pasul cu o asemenea irosire a resurselor, provocată de birocraţie, coduri de conduită, cazuri-test şi o mulţime de alte accesorii care însoţesc de obicei noua legislaţie. De la 9/11 încoace, atât în Marea Britanie, cât şi în Statele Unite s-au emis un număr enorm de noi legi. Marea Britanie a adoptat Legea de prevenire a actelor teroriste, iar Statele Unite – Actul Patriotic. Ambele seturi de legi au apărut odată cu dovezi vădite de intensificare a măsurilor de securitate, ceea ce include şi o supraveghere mai accentuată a populaţiei. Obligate să se confrunte cu fanatici care, ni se spune, ucid fără milă şi la întâmplare, ambele guverne au declarat că trebuie să adopte legi mult mai dure, pentru a se asigura că ucigaşii sunt luaţi de pe străzi şi ţinuţi departe de societate.

Această legislaţie este, în orice caz, foarte controversată. Cum adesea nu există suficiente dovezi pentru a garanta condamnarea unor suspecţi de terorism, noile legi permit statului să închidă cetăţenii fără a le asigura un proces corect. De aceea, ele sunt privite ca fiind neliberale şi împotriva vechilor tradiţii americane şi britanice. Inerente acestor legi sunt răspândirea colectării şi a stocării informaţiilor personale şi a spionării cetăţenilor.

În Marea Britanie, Legea protecţiei datelor şi Legea libertăţii informaţiei au fost adoptate pentru a ne proteja şi, cel puţin la nivel teoretic, pentru a ne asigura dreptul de a şti precis ce informaţii cu privire la noi înşine sunt deţinute de alte persoane. Cât de protejaţi ne fac să ne simţim toate acestea?

Administraţia Bush, a susţinut întruna că „transformăm salvarea vieţii americanilor într-o prioritate" şi a încercat să transforme Statele Unite într-o fortăreaţă, aruncând la gunoi, în timpul procesului, cartea drepturilor cetăţeneşti. Brutalitatea împotriva deţinuţilor arabi de la Abu Ghraib şi nu numai reprezintă o politică deliberată. Secretarul apărării Donald Rumsfeld a subliniat foarte clar că Armata Statelor Unite va întreprinde orice este necesar pentru a obţine informaţii de la orice persoană despre care se crede că ar putea deţine informaţii privind un eventual atac asupra Statelor Unite. Umilirea sexuală a arabilor este o metodă eficientă de constrângere. Societatea arabă consideră adesea că victima unei torturi de natură sexuală este singura răspunzătoare pentru soarta ei. Astfel, revelarea abuzului în faţa comunităţii din care face parte victima este mai dăunătoare decât abuzul în sine. Bărbaţii şi femeile răspunzători pentru abuz ori au respectat nişte ordine, ori au dezvăluit latura întunecată şi violentă a sufletului american.

De curând, în timp ce hoinăream pe străzile din Manhattan, m-am oprit într-o cafenea Starbucks şi am luat un exemplar din *New York Times*. Am citit că CIA a recunoscut că a torturat prizonieri în Irak şi în alte părţi ale globului, precum şi că Ministerul Justiţiei a cercetat un număr de cazuri în care deţinuţii au murit în timpul detenţiei ca urmare a interogatoriilor Agenţiei. P.J. Gross, directorul CIA, a declarat în faţa Congresului, în martie 2005, că toate interogatoriile se făceau în condiţii legale „în momentul actual". Când i s-a cerut, sub presiune, să facă aceeaşi declaraţie categorică în ceea ce priveşte tehnicile de interogare pe toată perioada scursă de la 11 septembrie

2001, el a refuzat să dea curs cererii. O expertiză juridică emisă de Ministerul Justiţiei în 2002 respecta o definiţie restrânsă a torturii. Acest fapt permitea Agenţiei să recurgă la o gamă largă de practici coercitive împotriva persoanelor suspectate de terorism, încarcerate în locuri ţinute secrete pe tot cuprinsul globului, fără a fi vinovată de „tortură". În orice caz, CIA a utilizat metode de interogare considerabil mai brutale decât cele ale altor agenţii militare sau civile. Iar folosirea tehnicii „transferului" de către CIA, ceea ce presupune predarea deţinuţilor autorităţilor din ţări ca Egipt sau Siria, recunoscute pentru utilizarea unei game largi de tehnici de constrângere mentale şi fizice, a fost acoperită de către presă. CIA pare că priveşte trimiterea suspecţilor către ţări din lumea a treia, spre a fi brutalizaţi, drept un mijloc de a rămâne cu mâinile curate.

„Actul Patriotic" din Statele Unite a intrat în vigoare în timpul perioadei de haos imediat următoare evenimentelor de la 11 septembrie. El a trecut de Congres în grabă, fără o dezbatere adecvată, la doar trei săptămâni de la tragedie. A fost semnat de preşedintele Bush pe 26 octombrie 2001, fără nici un raport al Camerei sau al Senatului. Este, oricum l-ai privi, un act legislativ draconic, în care expresia „act patriotic" este exprimarea specifică relaţiilor publice preferată „Actului de unificare şi întărire a Statelor Unite prin furnizarea de mijloace care să intercepteze şi să împiedice actele teroriste". Legea este o versiune de compromis a Actului antiterorism din 2001 şi a introdus zeci de schimbări constituţionale pentru a creşte puterile operaţionale ale agenţiilor de spionaj şi de impunere a legii. Ea conţine prevederi care extind drepturile statului de a monitoriza şi intercepta schimburi de informaţii private şi chiar dă FBI-ului acces la înregistrările vânzărilor de cărţi sau la datele bibliotecilor privind împrumuturile, din care specialiştii îşi pot forma păreri cu privire la convingerile politice ale cetăţenilor.

„Actul Patriotic" permite guvernului Statelor Unite să intercepteze informaţii transmise prin internet sau să limiteze libertăţile cetăţenilor cu ajutorul noilor tehnologii. El permite, de asemenea, agenţiilor specializate folosirea tehnologiilor de comunicare ultramoderne, fără a raporta Congresului, iar această stare de fapt are grave implicaţii pentru cetăţeni ai unor ţări din afara Statelor Unite, în principal Canada şi Marea Britanie. Actul conţine multe prevederi privind supravegherea electronică, prevederi care fuseseră propuse înainte de distrugerea turnurilor gemene şi care au fost, la vremea respectivă, subiectul unor dezbateri şi critici aprinse. Una dintre consecinţele evenimentelor de la 11 septembrie este imediata reducere la tăcere a oricărei opoziţii semnificative provocate de implicaţiile asupra libertăţilor cetăţeneşti pe care le-ar putea avea măsurile antiterorism. Administraţia Bush a tensionat şi mai mult atmosfera, precizând că are informaţii conform cărora alte atacuri asemănătoare sunt iminente şi că, fără „Actul Patriotic", guvernul ar fi paralizat şi incapabil să riposteze. Procurorul General John Ashcroft le-a acordat membrilor Congresului doar o săptămână pentru a dezbate şi a adopta legea, precizând că, dacă nu o fac, vor purta răspunderea pentru viitoarele atrocităţi comise de terorişti. John Podesta, şeful personalului de la Casa Albă între 1998 şi 2001, a remarcat că atitudinea Congresului s-a transformat, peste noapte, din precauţie extremă în consimţirea de a permite forţelor de impunere a legii „reîntoarcerea la o eră în care ele puteau monitoriza şi hărţui civili care pur şi simplu îşi exercitau drepturile stipulate în Primul Amendament".

Un singur senator, Russ Feingold, s-a opus Actului în perioada de haos de după 9/11. El s-a declarat convins că acordarea de puteri crescute agenţiilor în ceea ce priveşte supravegherea electronică nu va duce la o exercitare adecvată a acestora. „Dacă proiectul de lege îi acordă Procurorului General puteri sporite în ceea ce priveşte relaţia cu imigranţii, cine credeţi că

vor fi cei care vor suporta abuzurile provocate de aceste puteri? Nu imigranţii din Irlanda, El Salvador sau Nicaragua, nici măcar cei din Haiti sau Africa. Vor fi cei din ţările arabe, musulmane sau din sudul Asiei. Guvernul nostru a primit noi puteri imense şi efectul lor va cădea cel mai puternic pe umerii unei minorităţi a populaţiei noastre, cei care simt deja foarte acut consecinţele acestui dezastru de la 11 septembrie."

Ar fi incorect să las impresia că monitorizarea comunicaţiilor electronice din întreaga lume a fost privită de către Statele Unite drept o responsabilitate doar a lor. Guvernul Statelor Unite a făcut presiuni asupra tuturor democraţiilor pentru ca acestea să-şi perfecţioneze legile privind interceptarea comunicaţiilor, în aşa fel încât tehnologiile noi să fie încurajate. Terorismul reprezintă o problemă globală, prin urmare orice iniţiativă împotriva lui trebuie să aibă o dimensiune la fel de globală. Curând după 9/11, fostul director FBI Louis Freeh a primit din partea administraţiei Bush însărcinarea de a vizita ţări în curs de dezvoltare din Europa de Est, Asia şi Africa, pentru a promova ideea interceptării comunicaţiilor. Statele Unite au susţinut, de asemenea, necesitatea garantării ca toate tehnologiile de interceptare să fie prevăzute cu un sistem de supraveghere. Cu alte cuvinte, scopul era să prevină şi să facă ilegală fabricarea oricăror echipamente de comunicare sau de supraveghere care, la rândul lor, să nu poată fi spionate şi înregistrate.

Majoritatea ţărilor democratice îşi dau foarte bine seama, cu toate acestea, că a trage cu urechea la cetăţenii lor reprezintă o politică deloc populară şi în nici un caz dezirabilă din partea statului, prin urmare, au inclus în legislaţiile şi constituţiile lor măsuri de protecţie. Marea Britanie, Statele Unite şi majoritatea celorlalte democraţii sunt obligate prin lege să publice anual numărul interceptărilor comunicaţionale autorizate. Aceste ţări au regulamente ferme care prevăd ca interceptările să fie autorizate de către un judecător, şi asta numai după ce o serie de

condiţii stricte au fost respectate. Agenţiile de spionaj şi cele de impunere a legii nu au – cel puţin teoretic – permisiunea de a iniţia activităţi de interceptare înainte de a demonstra că alte metode de investigare au fost încercate, dar s-au dovedit ineficiente. Franţa şi Marea Britanie au înfiinţat comisii independente pentru a monitoriza abuzurile. Membrii acestor comisii au o înaltă calificare în utilizarea echipamentelor de comunicare şi a tehnologiilor de interceptare, precum şi puterea de a cerceta toate părţile implicate în supraveghere şi – lucrul cel mai important – pentru a pune întrebări incomode. Alte ţări, cum ar fi Canada, au numit Comisari ai Vieţii Private care au tocmai sarcina de a examina utilizarea corectă sau abuzivă a supravegherii de către stat.

Unele ţări publică anual rapoarte cu privire la utilizarea supravegherii de stat de către diverse departamente guvernamentale. Printre aceste ţări se numără Australia, Franţa, Canada, Noua Zeelandă, Elveţia, Suedia, Statele Unite şi Marea Britanie. Însă altele nu sunt la fel de dornice să-şi facă publice cifrele. Olanda, de exemplu, şi-a relaxat de curând legile privind raportarea interceptărilor de comunicaţii. La suprafaţă, faptul că o ţară cu o îndelungată tradiţie liberală precum Olanda face aşa ceva poate părea foarte ciudat. Dar de la asasinarea omului politic liberal Pim Fortuyn şi a regizorului radical Theo Van Gogh atitudinea olandezilor cu privire la extremismul islamic din ţara lor s-a înăsprit. Faptul că Olanda este ţara cu cel mai mare procentaj de imigranţi, legali şi ilegali, şi totodată ţara cu cea mai multe interceptări din Uniunea Europeană nu este probabil o coincidenţă. Pe măsură ce tot mai multe ţări intră în UE, permiţând tot mai multor non-cetăţeni să pătrundă în statele membre – Turcia, prima ţară cu adevărat musulmană, abia aşteptând să fie admisă –, se înregistrează o atitudine explicabilă de respingere tot mai mare din partea ţărilor preponderent creştine, care vor să ridice bariere

în calea a ceea ce se tem că ar putea deveni o cucerire culturală şi religioasă.

Responsabilitatea instanţelor de monitorizare care controlează supravegherile nu presupune cercetarea doar a interceptării de informaţii în statele de care ţin, ci şi a tuturor supravegherilor electronice efectuate la nivel global. Posturile de ascultare ale sediului guvernamental de comunicaţii din Cheltenham şi agenţia americană de la Menwith Hill, din Yorkshire, „trag cu urechea" în toată lumea şi aproape că nu există democraţie care să nu aibă o agenţie secretă cu funcţii asemănătoare.

Listele publicate ale operaţiunilor de supraveghere furnizează informaţii cu privire la tipul de supraveghere electronică utilizat şi precizează şi durata pe care acestea au fost active. Justificarea principală pentru asemenea monitorizări are două capete de afiş: infracţiunile şi terorismul. Listele supravegherilor sunt publicate pentru a demonstra că activităţi acceptabile, precum investigaţiile jurnalistice, activismul ecologic, drepturile omului, sindicalismul, activităţile religioase şi opoziţia politică sunt scutite de la supravegherea fără mandat şi că aceste grupuri nu reprezintă o ţintă doar pentru că ar putea avea conflicte de interese cu cei de la putere. Trebuie, de asemenea, precizat că infracţiunile minore nu pot fi subiectul supravegherii intruzive din motive politice. A face agenţiile de siguranţă să dea socoteală electoratului monitorizându-le activităţile este un aspect vital într-o adevărată democraţie.

Nu trebuie să fii adept al teoriei conspiraţiei pentru a avea îndoieli în ceea ce priveşte abuzurile făcute de stat în supravegherea electronică şi interceptarea corespondenţei. Articolul 17 din Carta Drepturilor Omului cere ca „integritatea şi confidenţialitatea corespondenţei să fie garantate, *de jure* şi *de facto*. Corespondenţa trebuie livrată destinatarului fără a fi interceptată şi deschisă sau citită printr-o altă metodă. Supravegherea, indiferent dacă este electronică sau făcută prin alte mijloace,

interceptarea de mesaje telefonice, telegrafice sau de alt fel şi înregistrarea conversaţiilor trebuie interzise".

Serviciul de Securitate britanic a înregistrat un total de 540 de interceptări în 2004. Cu toate acestea, dezbaterea cu privire la proiectul de lege antiterorism a arătat că interceptările efectuate în scopul de a impune legea au fost constante şi larg răspândite în Marea Britanie. Faptul că persoanele suspectate de terorism erau încarcerate fără proces şi fără a fi informate de acuzaţiile care li se aduc era, potrivit ministrului de interne David Blunkett, justificabil din motive de securitate. Cu alte cuvinte, dacă un suspect ar şti pe baza căror dovezi a fost închis, el şi-ar putea da seama de modul în care serviciile de siguranţă au obţinut informaţiile respective. „Interceptările nu pot fi folosite ca dovezi în instanţă şi eu nu sunt pentru permiterea utilizării lor", a declarat Blunkett. Adevărul este că majoritatea interceptărilor efectuate de serviciile de siguranţă sunt în afara legii, iar persoanele care le efectuează nu au nici cea mai mică dorinţă să-şi justifice acţiunile în faţa unui judecător.

Această reticenţă lipseşte cu desăvârşire în Statele Unite. „Actul Patriotic" este foarte nepopular în multe părţi ale Statelor Unite, din cauza modalităţilor în care eludează prevederile adoptate tocmai pentru preveni folosirea abuzivă a supravegherii cetăţenilor de către stat. În februarie 2004, consiliul oraşului New York a adoptat o rezoluţie ce condamna încălcarea drepturilor la viaţa privată garantate de Constituţie. Autorii şi bibliotecarii au protestat faţă de secţiunea a cincea a Actului, care permite verificarea înregistrărilor bibliotecilor. Gama de puteri acordate FBI-ului a crescut în mod vizibil din anul în care Actul a intrat în vigoare. Numărul de mandate ce permiteau supravegheri a crescut în 2004, depăşind 2 000, deci cu mult mai multe decât mandatele federale emise. Acest lucru este cauzat de faptul că „Actul Patriotic" a făcut supravegherea oamenilor inocenţi mult mai simplu de justificat. Şi autorităţile canadiene au fost foarte preocupate de

această problemă. În noiembrie 2004, comisarul responsabil cu protecţia vieţii private din British Columbia a prezentat un raport ce sugera că informaţii personale despre cetăţeni canadieni au fost obţinute de către autorităţile americane sub protecţia Actului, ceea ce violează drepturile canadiene la viaţa privată. Plângeri referitoare la interceptarea şi analizarea schimburilor de informaţii între cetăţeni britanici, ajutate şi sprijinite de către compania British Telecom şi controlate de către Agenţia Naţională de Securitate (NSA) la Menwith Hill, s-au lovit de o nepăsare totală.

Implicaţiile detaliate ale puterii crescânde a statului au devenit din ce în ce mai evidente pe măsură ce publicul a început să realizeze ce se întâmplă. Există trei legi în cadrul Actului care se referă la interceptarea comunicaţiilor de către guvernul Statelor Unite. Titlul III, referitor la interceptarea convorbirilor telefonice şi la interceptarea în timp real a comunicaţiilor tip voce sau date, stipulează existenţa unei „cauze probabile“ şi aprobarea unui judecător. Este o precauţie importantă, care necesită implicarea unei persoane aflate pe o treaptă înaltă a sistemului juridic. Legea privind confidenţialitatea comunicaţiilor electronice (ECPA) reglementează instalarea de aparate pen-register (care colectează numerele apelate de la un anumit post telefonic) şi folosirea unor sisteme de tip „interceptează şi urmăreşte“ (care înregistrează numerele ce apelează un anumit post telefonic). Aceste echipamente pot fi folosite pentru a înregistra întreaga activitate pe internet a unei persoane fizice care foloseşte o linie telefonică. Acest Act nu presupune necesitatea unei „cauze probabile“, iar pentru utilizarea dispozitivelor nu este nevoie decât de un ordin judecătoresc, care poate fi obţinut de un avocat guvernamental. Pentru a-l obţine, acesta nu trebuie decât să garanteze verbal curţii că informaţiile sunt relevante în cadrul unei investigaţii în desfăşurare. Astfel, Actul face foarte simplă pentru guvern accesarea informaţiilor financiare private, fără a trebui să prezinte dovezi că persoana afectată de acest

abuz este suspectată de implicare într-o activitate criminală. O a treia lege, „Legea supravegherii serviciilor secrete străine", permite utilizarea supravegherii electronice în cazul oricărei persoane care se află în Statele Unite şi despre care se crede că ar fi agentul unei puteri străine. Supravegherea necesită numai o „cauză dreaptă" şi un ordin judecătoresc, dar îi oferă persoanei fizice o protecţie mai puţin consistentă decât în cazul ascultării telefoanelor. Asemenea situaţii apar când informaţii cu privire la cetăţeni britanici, obţinute de americani pe teritoriu britanic, sunt împărtăşite cu serviciile secrete britanice.

Diferenţa dintre Titlul III şi Legea privind confidenţialitatea comunicaţiilor electronice este că primul priveşte conţinutul comunicaţiilor, în timp ce ECPA şi utilizarea „înregistratoarelor-stilou" şi a sistemelor „interceptează şi urmăreşte" privesc, teoretic, doar nişte cifre. În consecinţă, acordul judecătoresc poate fi obţinut în urma unei banale declaraţii a procurorului, iar procedura este foarte indulgentă cu prevederile ce protejează viaţa privată din Titlul III. Actul care s-a transformat în lege în octombrie 2001 a redefinit pen-register drept „un dispozitiv sau un proces cu ajutorul căruia se înregistrează sau decodează impulsuri reprezentând sau semnalând informaţii de la un instrument folosit pentru transmiterea unui conţinut informaţional de natură electronică" – ceea ce include şi e-mailurile trimise de pe un laptop. Un sistem de tipul „interceptează şi urmăreşte" a fost redefinit, în mod similar, ca „un dispozitiv sau un proces care captează impulsuri, electronice sau de altă natură, ce identifică o sursă de informaţii de la un instrument folosit pentru transmiterea unui conţinut informaţional de natură electronică". Aceste „redefiniri" sunt semnificative, pentru că ele permit autorităţilor să intercepteze şi să stocheze imense cantităţi de informaţii private, fără acordul unui judecător, pe baza unei simple declaraţii a unui procuror. Interceptarea poştei electronice, a paginilor accesate cu ajutorul browserelor şi a altor forme

de comunicare electronică este cunoscută sub numele de „Carnivore" şi formează nucleul central al „Actului Patriotic". Ea este responsabilitatea FBI-ului. Datele pe care Biroul le colectează şi analizează sunt, desigur, mult mai consistente decât nişte simple numere de telefon, din moment ce pot fi monitorizate site-uri sau alte informaţii accesate cu ajutorul internetului.

În iulie 2000, Procurorul General al Statelor Unite a creat Consiliul de Supraveghere al Departamentului de Justiţie, al cărui rol este examinarea problemelor privind intimitatea şi drepturile cetăţeneşti generate de „Carnivore". În orice caz, când George W. Bush a fost ales preşedinte, Consiliul a fost înlocuit de un „oficial de nivel înalt". Raportul nu a fost terminat până la 11 septembrie 2001 şi, deloc surprinzător, Congresul nu a putut beneficia de rezultatul cercetărilor atunci când a trebuit să adopte, sub presiune, „Actul Patriotic".

Pe lângă evidenta natură deloc liberală a Actului, acesta mai are şi o alarmantă aură de iresponsabilitate. Pe de-o parte tolerează şi încurajează agenţiile de impunere a legii care interceptează comunicaţiile şi monitorizează cetăţenii Statelor Unite, ai Canadei şi ai Marii Britanii, şi pe de altă parte cedează în faţa lobby-ului în favoarea armelor de foc şi, cel puţin aparent, pune interesele posesorilor de arme înaintea sfaturilor agenţiilor antiteroriste, acestea nemaiputând interveni atunci când suspecţii de acte teroriste îşi cumpără arme. În Statele Unite, grupările fundamentaliste islamice, miliţiile radicale şi alte grupuri recunoscute că recurg la mijloace violente pentru a-şi promova cauzele au dreptul de a cumpăra arme după bunul lor plac. A-l nega este neconstituţional şi o serioasă încălcare a drepturilor lor. Legea precizează că singurele grupuri care nu au voie să cumpere arme sunt criminalii condamnaţi, imigranţii ilegali şi persoanele cu tulburări mentale. Asociaţia Naţională pentru Arme de Vânătoare face unul dintre cele mai puternice lobby-uri din Statele Unite şi este un apărător fără scrupule al

dreptului de a purta armă. Senatorul democrat din New Jersey, Frank Lautenberg, acuza administraţia Bush că apleacă prea mult urechea la lobby-ul armelor de foc, acest interes concretizându-se în anomalii apărute în înregistrările cu privire la posesorii de arme; senatorul cere acţiune imediată. Conform FBI-ului, agenţii săi nu au permisiunea de a accesa sau folosi informaţii despre posesorii de arme şi nu au voie să ia măsuri atunci când persoanele suspectate de terorism cumpără arme de foc. Fostul procuror general John Ashcroft nu a permis FBI-ului să compare lista persoanelor suspecte de terorism cu lista celor care au achiziţionat arme de foc. „Lista teroriştilor sub supraveghere" a FBI-ului reuneşte câteva mii de suspecţi despre care nimeni nu ştie câte arme au achiziţionat din 2001 încoace. Nu se ştie decât că cel puţin 47 au primit permise de portarmă în cele nouă luni de după iunie 2004. Conform FBI-ului, toate aceste persoane erau terorişti fie dovediţi, fie suspecţi, şi se aflau pe lista monitorizărilor permise de „Actul Patriotic". Astfel, regulile se întorc împotriva FBI-ului, care este obligat prin lege să distrugă orice informaţii cu privire la posesorii de arme de foc în cel mult 24 de ore de la obţinerea acestora.

Legea prevenirii actelor de terorism din Marea Britanie a primit acordul regal pe 11 martie 2005, după un traseu dificil prin Parlament. Legea a introdus un sistem de ordine ale ministrului de interne menite să anihileze activităţile teroriste. Aceste ordine de control permit ministrului să interzică persoanelor suspectate de activităţi teroriste asocierea cu anumite persoane, folosirea internetului sau a telefoanelor mobile, şi să le restricţioneze deplasările. Suspecţii pot fi urmăriţi şi supuşi arestului la domiciliu. Este o lege dură şi neliberală, pentru că se aplică tuturor cetăţenilor britanici şi anulează prezumţia de nevinovăţie. Cu toate acestea, există şi măsuri de precauţie. Ministrul de interne trebuie să apeleze la un judecător de la Curtea Supremă pentru a putea da un ordin de control care nu se abate de la lege,

deşi, dacă este urgent, poate sări peste acest pas iniţial, având obligaţia de a cere confirmarea Curţii în termen de şapte zile. În practică, ministrul de interne poate forţa o persoană să rămână în arest la domiciliu, o decizie neconformă cu hotărârile Curţii Europene a Drepturilor Omului, dar această decizie trebuie confirmată, după dezbatere, de Parlament în cel mult 40 de zile. Puterile ministrului de interne sunt descrise ca temporare şi pot fi pierdute după un an, dacă el nu primeşte un nou vot de încredere din partea ambelor camere ale Parlamentului. Măsurile de prevedere includ şi numirea unui supervizor independent, care trebuie să prezinte un raport Parlamentului, în fiecare an, despre modul în care a fost respectată legea şi despre utilizarea ordinelor de control. Proiectul de lege pentru prevenirea terorismului a intrat în vigoare numai pentru că s-a sincronizat cu ceea ce era considerată o criză de securitate fără precedent în Marea Britanie. Întrebarea este cât va dura până când legea va fi abrogată şi ţara se va întoarce la normal. Mare parte din legile antiterorism intrate în vigoare în trecut au avut tendinţa să rămână în vigoare ani de zile, dacă nu chiar pe termen nedefinit.

Oricine a încercat să citească Legea protecţiei datelor din 1998 va observa cât de dificil este să înţelegi exact cum o poţi utiliza pentru a-ţi proteja propria viaţă privată. Actul din 1998 este o actualizare a unei legi din 1984 şi a intrat în vigoare după dezbateri îndelungate în Parlament. Era deja, lucru cât se poate de previzibil, depăşită chiar în momentul intrării în vigoare, din cauza progresului tehnologic foarte rapid. Legea are un comisar al Informaţiilor pentru a i se asigura respectarea şi permite recursul la Legea drepturilor omului. Acest amănunt nu numai că ajută persoanele fizice, dar joacă şi un rol major în modul în care prevederile legii sunt interpretate şi puse în aplicare în momentul când un caz ajunge în faţa Curţii. Există un cod de bune practici ce însoţeşte legea, iar avocaţii pot câştiga sume foarte mari reprezentând în instanţă persoane care consideră că le-a fost violată

intimitatea. La o primă vedere, nu pare să se stipuleze în lege că un şofer ar trebui avertizat dacă maşinii pe care o conduce i se ataşează un dispozitiv de urmărire. De asemenea, nu se limitează nici modul în care sunt folosite informaţiile obţinute de către supraveghetori. Care este poziţia legală a unei organizaţii care strânge imagini cu clienţii băncilor în timpul utilizării bancomatelor, dacă aceste imagini sunt furate de o bandă de hoţi?

În esenţă, Legea protecţiei datelor acoperă orice informaţie privată care este colectată sau înregistrată, electronic sau pe hârtie. De exemplu, de fiecare dată când furnizezi informaţii personale unui site, cum ar fi adresa de poştă electronică, adresa poştală, vârsta sau numărul de telefon, site-ul respectiv este obligat, din punct de vedere legal, să te anunţe în ce scop are nevoie de aceste informaţii şi, în acelaşi timp, este obligat să-ţi dea posibilitatea de a decide dacă poate furniza datele tale unei terţe părţi. Ar trebui să-ţi ofere o înştiinţare privind folosirea informaţiilor, ca să precizeze scopul în care este nevoie de datele tale. Când o persoană se abonează la o revistă sau completează un cupon dintr-o reclamă, de obicei ea poate opta să primească informaţii de la organizaţii „partenere" în scopuri de marketing (lucruri scrise de obicei cu litere foarte mici). Dacă abonatul refuză, este ilegal ca la datele sale să mai aibă acces altcineva. Organizaţiile comerciale pot utiliza datele numai în scopul stipulat în contract. Site-urile trebuie să precizeze dacă informaţia furnizată lor va fi codată. Şi, dacă o bază de date colectează informaţii personale, ea este obligată să păstreze informaţia respectivă pe o durată cât mai scurtă posibil, deşi această durată nu este întotdeauna reglementată legal.

Toate neplăcerile provocate de reclamele nedorite pe care le primim pe e-mail pornesc de la cedarea detaliilor noastre personale, în mod ilegal, către o companie de marketing. Legea protecţiei datelor are scopul de a proteja toate informaţiile personale, de la detalii bancare până la înregistrări ale Serviciului

Naţional de Sănătate (NHS), adrese de e-mail sau numere de telefon. Cetăţenii unei ţări au dreptul de a vedea toate informaţiile strânse despre ei de către o organizaţie publică sau privată. Companiile comerciale trebuie să justifice păstrarea acestor informaţii. Dacă nu o fac, păstrarea este ilegală, iar informaţiile trebuie şterse, conform legii. Datele cerute de cetăţeni trebuie furnizate cu cel puţin 40 de zile înainte ca aceştia să poată face reclamaţie la comisarul Informaţiilor.

Legea protecţiei datelor mai reglementează şi ce poate sau nu poate fi făcut în domeniul, aflat în rapidă dezvoltare, al supravegherii. În Marea Britanie, sunt patru tipuri de supraveghere nereglementate prin lege. Mai întâi, este vorba de activităţile de supraveghere intruzive, acoperite de Legea reglementării puterilor de investigare, care se ocupă de antiterorism şi infracţiuni grave. Apoi, supravegherea angajaţilor de către companii care vor să se asigure că personalul se supune contractului semnat la angajare. Al treilea tip este reprezentat de supravegherea cu ajutorul echipamentelor de securitate instalate de proprietari în locuinţele lor. În sfârşit, camerele de filmat şi echipamentele similare utilizate pentru a transmite imagini în scopuri jurnalistice, artistice sau literare. Legea din 1998 stipulează o serie de standarde de bază. Datele înregistrate prin CCTV trebuie procesate, conform legii, numai în scopuri limitate şi în concordanţă cu drepturile omului, trebuie să fie adecvate şi relevante, să dea dovadă de acurateţe şi să nu fie stocate mai mult decât este necesar. De asemenea, nu este permis ca ele să fie transferate către ţări care nu oferă prin lege o protecţie adecvată a datelor.

Comisarul Protecţiei Datelor poate emite preavize de constrângere dacă el sau ea consideră că s-a produs o încălcare a legii. Codul de bune practici intră în posesia oricărei persoane care instalează echipament de supraveghere. El trebuie să fie revăzut în mod regulat, pentru a se lua în consideraţie schimbările în interpretarea legislaţiei, în tehnologia pentru înregistrarea

imaginilor ori a sunetelor, tehnicile de recunoaştere facială şi tehnologia digitală, toate acestea fiind tratate în lege.

Când un sistem CCTV este instalat, utilizatorii trebuie să justifice necesitatea acestuia. De exemplu, ei pot fi interesaţi de prevenirea, investigarea şi detectarea unei infracţiuni, de arestarea şi punerea sub urmărire a infractorilor, de siguranţa personalului şi de cea publică sau de monitorizarea securităţii unei locuinţe. Reprezintă o infracţiune instalarea unui sistem ce nu respectă măsurile de siguranţă stipulate prin lege. Persoanele implicate în instalarea sistemului trebuie să se legitimeze şi să dea o declaraţie cu privire la importanţa utilizării CCTV sau a oricărui alt echipament de supraveghere. Vor trebui să-şi justifice opinia şi să enumere motivele instalării. Scopurile vor fi aduse la cunoştinţa Oficiului pentru Protecţia Datelor. De asemenea, trebuie precizate persoanele care se vor asigura că funcţionarea zilnică a echipamentelor este în conformitate cu codul de bune practici, precum şi cu regulile de securitate a documentelor şi de confidenţialitate. Modul în care imaginile sunt înregistrate trebuie de asemenea să fie în conformitate cu legea, iar echipamentul trebuie instalat într-un loc din care va putea monitoriza numai zona ce se intenţionează a fi acoperită. Dacă există spaţii private în apropierea echipamentelor, utilizatorul va trebui să discute instalarea cu proprietarii spaţiilor respective, pentru a obţine acordul lor în cazul în care există o cât de mică posibilitate ca echipamentul să înregistreze imagini din acea zonă.

Operatorii sunt obligaţi să folosească echipamentul numai pentru scopurile pentru care acesta a fost instalat. Multe sisteme CCTV, cum ar fi cele folosite în centrele oraşelor sau lângă hipermarketuri, sunt adesea foarte sofisticate şi tind să îndrepte camerele de luat vederi spre anumite activităţi, să focalizeze pe anumite persoane, să examineze imagini deja înregistrate pentru a găsi delincvenţi sau martori, sau pentru a observa comportamentul unui angajat. Organizaţiile ce folosesc CCTV pentru orice

altceva decât cea mai banală supraveghere trebuie să respecte legea, dar nu toate imaginile lor vor putea fi acoperite în toate circumstanţele. Regula de bază este că posesorii sistemului sunt singurii care decid dacă imaginile înregistrate îi fac să afle o informaţie specifică despre activităţile unei anumite persoane.

În cazul în care camerele sunt reglabile, operatorii nu au voie să le manipuleze pentru a ajunge la zone ce nu au fost precizate dinainte. Dacă restricţionarea zonelor de acces ale camerei, pentru a respecta dreptul la intimitate, este imposibilă, operatorii trebuie învăţaţi să recunoască implicaţiile încălcării vieţii private de către ceea ce filmează. De exemplu, persoanele care fac plajă în grădina din spatele casei se aşteaptă mai mult să aibă intimitate decât cele care tund gazonul în grădina din faţă. Este în regulă ca scopul unui echipament să fie protejarea persoanelor care folosesc un bancomat, dar este ilegal să înregistrezi imagini cu codurile PIN şi situaţia conturilor.

Semne vizibile şi uşor de citit trebuie aşezate în zone uşor accesibile publicului, pentru ca acesta să vadă că zonele respective se află în raza unui echipament de supraveghere. Există reguli clare despre dimensiunea semnelor: ele trebuie să identifice beneficiarul supravegherii, de ce se află echipamentul acolo şi persoana de contact pentru mai multe informaţii. Uneori sistemul de supraveghere poate fi mutat fără avertisment – de exemplu, în cazul în care anunţarea prezenţei camerelor de supraveghere periclitează o investigaţie. În acest caz, sistemul trebuie să fie demontat imediat ce nu mai este necesar.

Există reguli stricte şi în ceea ce priveşte calitatea imaginilor obţinute. Dacă un sistem a fost instalat pentru a detecta sau preveni o infracţiune, imaginile trebuie să fie adecvate, să fie testate cu regularitate şi să fie conforme cu normele de calitate specificate în lege. Un „monitor uman“ trebuie să se afle la faţa locului pentru a decide cum trebuie procedat într-o situaţie specifică. Declaraţiile persoanei respective trebuie înregistrate. Dacă

infracţiunea investigată prin această formă de supraveghere are loc noaptea, atunci înregistrarea constantă poate fi realizată doar la momente dinainte specificate, cu camere bine întreţinute. Pe durata păstrării imaginilor, integritatea lor trebuie menţinută, pentru a asigura valoarea de dovadă şi pentru a proteja drepturile persoanelor ale căror imagini au fost înregistrate. Legea precizează că aceste imagini nu trebuie păstrate mai mult decât este necesar. De pildă, dacă nu sunt necesare ca dovezi, imaginile înregistrate în centrul oraşelor trebuie şterse după 31 de zile. Vizionarea acestor imagini ar trebui să se facă în locuri restricţionate, doar în faţa persoanelor care fac parte din personal. Există prevederi stricte cu privire la depozitarea filmelor care ar putea fi folosite ca dovezi la tribunal. Aceste reguli vizează şi asigurarea că drepturile indivizilor înregistraţi sunt protejate. Orice hotărâre de a face publice imaginile trebuie să respecte legea.

Dacă scopurile sistemului sunt prevenirea şi descoperirea infracţiunilor, atunci cedarea imaginilor către terţe părţi se poate face numai către agenţii de impunere a legii, către reprezentanţi legali şi mass-media (când este nevoie de ajutorul publicului pentru a identifica victima), către un martor sau un infractor implicat în infracţiune sau către oamenii ale căror imagini au fost înregistrate şi depozitate.

Există opt principii pentru protejarea datelor. Acestea sunt precizate în lege şi trebuie respectate de orice persoană implicată în supravegherea publicului. Există şi un Controlor de Date, care răspunde, în conformitate cu Legea protecţiei datelor, de iniţierea supravegherii. Desigur, Controlorul nu are nici o influenţă asupra supravegherilor iniţiate pe ascuns sau asupra interceptărilor de conversaţii. O privire aruncată pe site-urile de unde se poate achiziţiona echipament de spionaj arată că există o gamă largă de produse pentru cei care vor să tragă cu urechea. O gamă ce se îmbunătăţeşte zi de zi. Şi care nu intră sub incidenţa nici unei legi.

CAPITOLUL IX

Rateurile serviciilor secrete

În ciuda rateurilor agenţiilor de spionaj care au făcut posibil atentatul din 11 septembrie, serviciile secrete britanice şi americane sunt în continuare incapabile să ţină pasul cu evenimentele naţionale. O Comisie a Statelor Unite, înfiinţată pentru a monitoriza serviciile secrete, a raportat în aprilie 2005 două lucruri: comunitatea spionilor americani nu numai că s-a înşelat în totalitate în aproape toate concluziile pe care le-a tras înainte de Războiul din Irak, dar este în continuare în ceaţă în ceea ce priveşte stadiul actual al programelor nucleare ale statelor ostile – în ciuda faptului că presupusele ambiţii nucleare ale lui Saddam au fost unul din principalele motive oferite în favoarea pornirii unui război împotriva Irakului. Agenţii precum CIA, FBI, NSA şi nou-înfiinţatul Departament al Securităţii Interne se consideră în continuare mai degrabă rivali decât colaboratori cu aceeaşi misiune – aceea de a lupta împotriva terorismului mondial. Pentru mulţi observatori, un motiv şi mai mare de îngrijorare l-a reprezentat manipularea serviciilor secrete în perioada premergătoare invaziei din Irak.

Nici CIA, nici MI5 nu au reuşit să transmită factorilor politici de decizie îndoielile puternice pe care le aveau referitor la una din sursele-cheie de informaţie asupra presupuselor reserve de arme de distrugere în masă de care dispunea Irakul.

Poate că a sosit, în sfârşit, vremea când funcţionarii publici arată numai ceea ce cred ei că superiorii politici vor să vadă. Cazul teroristului algerian Kamel Bourgass, care a fost închis în 2005 pentru uciderea unui ofiţer de poliţie şi pentru punerea la cale a unor atentate teroriste, este considerat un exemplu al eşecului serviciilor secrete britanice şi al agenţiilor de impunere a legii, dar şi al altor departamente guvernamentale, inclusiv al serviciului de imigraţii. Din când în când, industria de asigurări face publică o estimare a riscurilor teroriste iminente. Ameninţările primesc calificative precum: „crescut“ (care e rău) şi „foarte crescut“ (care e şi mai rău). De exemplu, Marea Britanie are un risc „crescut“ de atac terorist de la începutul Războiului din Irak. Potrivit brokerilor internaţionali de asigurări de la Aon, există în prezent opt categorii de terorişti care ar putea ameninţa Occidentul, iar Marea Britanie este foarte aproape de capul mesei, confruntându-se cu cel puţin patru dintre acestea. Aon ne informează că suntem ameninţaţi de extremişti musulmani, grupări ale militanţilor pentru drepturile animalelor, grupări teroriste ale republicanilor irlandezi şi grupări ale crimei organizate. Şi Statele Unite se află sub ameninţare, dar lista lor de ameninţări include riscuri de atac din partea extremiştilor de dreapta şi a extremiştilor religioşi. Întrebarea cu care se confruntă publicul este: cât de mare e de fapt ameninţarea? Politicienii ne avertizează mereu că o nenorocire e pe cale să se-ntâmple, dar aceasta fie nu se petrece până la urmă, fie este cât pe ce să aibă loc, dar detaliile sunt trecute sub tăcere, pentru ca procesul legal să nu fie pus în pericol. Aşadar, ce se întâmplă de fapt? Ce să înţelegem din evenimentele recente?

În ciuda celor mai mari eforturi depuse de guvern, opinia publică britanică a început, inevitabil, să se blazeze în privinţa ameninţării teroriste. Aceasta se poate datora parţial faptului că sistemul judiciar penal britanic se asigură că orice informaţie care poate periclita un proces corect este ţinută departe de

domeniul public până la terminarea procesului legal. De la atacul din 11 septembrie, a existat o revărsare de „incidente“ teroriste pe teritoriul britanic şi, cu toate acestea, publicul a fost ţinut departe de ceea ce se petrecea în spatele cortinei. Pe fundalul unei îngrijorări publice generale pentru felul în care Ministerul de Interne se joacă cu drepturile cetăţeneşti, politicienii continuă să pună placa „pericolului mereu prezent“, avertizând că între Marea Britanie şi grupările fundamentaliste există o stare de război şi că ameninţarea teroristă rămâne iminentă. Deoarece nu au existat atrocităţi cu bombe pe străzi sau gazări în masă în metroul londonez, publicul a rămas protejat de ceea ce politicienii insistă să numească o falsă senzaţie de siguranţă şi fie nu acordă importanţă avertizărilor guvernului şi poliţiei, fie respinge aceste avertizări, considerându-le minciuni sau vorbe goale. Mulţi dintre noi îşi mai amintesc încă violenţele campaniei cu bombe purtate de IRA (şi unii dintre noi au luat contact direct cu ele), dar chiar şi amintirile noastre se estompează în timp, lăsând în urmă un aer de indiferenţă faţă de actuala ameninţare teroristă.

În Statele Unite, politicieni, printre care şi preşedintele Statelor Unite sau secretarul apărării Donald Rumsfeld, au vorbit despre terorişti Al Qaeda înarmaţi, umblând în libertate prin Europa, şi au făcut cumva o legătură între aceasta şi situaţia din Irak, pentru a-şi justifica decizia de a porni un război. Dar publicul britanic nu a avut nici un fapt pe baza căruia să-şi formeze o opinie. Motivul pentru această ignoranţă generală în ceea ce priveşte situaţia actuală a terorismului din Marea Britanie îl constituie seria de trei procese corelate care se aflau în derulare la Old Bailey (Curtea Penală Centrală) şi care s-au încheiat de-abia în primăvara lui 2005. Dacă mass-media ar fi avut acces la detalii înainte de încheierea procesului, acesta nu s-ar mai fi putut desfăşura corect. Lordul Cancelar a *emis un ordin pentru toate cele trei procese, care a interzis ori*ce comentariu legat de aceste subiecte. Abia în aprilie 2005 a

fost recunoscut în mod public că, între anii 2004–2005, Curtea Penală Centrală din Londra a fost într-o permanentă stare de alertă crescută, din pricina afirmaţiilor referitoare la planuri teroriste musulmane care au pătruns în sistem. S-au strâns tot mai multe dovezi care demonstrau că teroriştii plănuiau atacuri în toată capitala britanică, cu ajutorul explozibililor, al cocktailurilor cu gaze otrăvitoare, al ricinei şi al altor substanţe chimice toxice. Puţinii privilegiaţi care au urmărit în Old Bailey procesul intentat teroristului fanatic Kamel Bourgass şi complicilor lui s-au întrebat probabil de ce anume e nevoie pentru a convinge publicul britanic că se confruntă cu un mare pericol.

În primele două procese, au fost aduse acuzaţii împotriva a opt bărbaţi inculpaţi, dar au mai fost implicaţi cel puţin încă alţi şase, care n-au fost niciodată prinşi, şi câţiva activişti, ale căror detalii rămân necunoscute. Unii dintre acuzaţi erau terorişti bine pregătiţi, având legături cu taberele de antrenament Al Qaeda din Afganistan; ei frecventau moscheea din Finsbury Park din nordul Londrei, folosind-o drept centru de comandă pentru a purta războiul pe teritoriul britanic. Procesele nu numai că au dezvăluit pericolele cu care s-a confruntat publicul britanic după 9/11, dar au arătat în detaliu şi incapacitatea agenţiilor de apărare trimise să ancheteze şi să-i aresteze pe teroriştii implicaţi.

Nigel Sweeney, procuror al Coroanei în procesul Bourgass, a prezentat dovezi care demonstrau fără putinţă de tăgadă că moscheea Finsbury Park era un centru terorist unde erau copiate şi distribuite fundamentaliştilor din întreaga ţară reţete pentru ricină, gaze otrăvitoare şi explozibili. Reţetele au fost descoperite iniţial în Kabul, în timpul Războiului din Afganistan, şi nu erau altceva decât nişte încercări şcolăreşti de a fabrica otravă. Detalii ale celulelor teroriste, inclusiv fotografii, au fost descoperite după ce MI5 a primit un pont şi au fost folosite ca dovezi. La primul proces, în boxa acuzaţilor au fost

Kamel Bourgass, Mouloud Sihali, David Aissa Khalef, Sidali Feddag şi Mustapha Taleb. Acuzaţiile care le-au fost aduse au fost de complicitate la crimă şi plănuirea unor acţiuni periculoase la adresa populaţiei între 1 ianuarie 2001–23 ianuarie 2002. Toţi, cu excepţia lui Bourgass, au fost declaraţi nevinovaţi de acte teroriste. Bourgass era un tânăr de 27 de ani, licenţiat în ştiinţele naturii, şi un produs al taberelor de antrenament Al Qaeda din Afganistan, a cărui singură infracţiune anterioară fusese o condamnare pentru că furase dintr-un magazin trei perechi de blugi, în iulie 2002. Juraţilor le-au trebuit 15 ore ca să-l condamne pe Bourgass pentru moartea poliţistului Stephen Oake, pentru tentativă de omucidere împotriva a doi ofiţeri din Divizia Specială şi pentru vătămarea corporală premeditată a sergentului de poliţie Paul Grindrod. A fost condamnat la închisoare pe viaţă, plus alţi 17 ani, în paralel, pentru acte teroriste. Judecătorul procesului a recomandat ca Bourgass să petreacă cel puţin 30 de ani în închisoare, înainte de a fi putea fi eligibil pentru eliberare condiţionată. În timp ce îi citea sentinţa, judecătorul a comentat că 30 de ani e cea mai lungă condamnare pe care o poate da, deoarece noua lege penală, Criminal Justice Act, nu fusese încă promulgată. Dacă ar fi putut, ar fi ordonat ca Bourgass să fie închis pentru tot restul vieţii.

Acuzaţii în cel de-al doilea proces au fost: Khalid Alwerfeli, Samir Asli, Mouloud Bouhrama, Kamel Merzoug şi un al cincilea bărbat, Mohamed Meguerba, care a încălcat cauţiunea şi a fugit în Algeria. Toţi, cu excepţia lui Meguerba, au fost absolviţi de acuzaţia de terorism, dar condamnaţi pentru încălcarea legii imigrării. Cel de-al treilea proces nu a mai fost intentat. Nigel Sweeney a declarat în faţa instanţei: „Cel puţin zece musulmani ale căror nume sunt cunoscute, împreună cu persoane necunoscute, plănuiau să provoace moartea, rănirea sau înspăimântarea populaţiei britanice printr-un Jihad (război sfânt)". Toţi erau imigranţi ilegali din Algeria, trăind în locuinţe secrete

în Manchester, Londra, Doncaster şi Bournemouth. Punerea la cale a unui atac terorist „spectaculos" a început în ianuarie 2001, dar descoperirea care a salvat Londra de violenţe grave n-a avut loc decât doi ani mai târziu, în ianuarie 2003, când ofiţeri antitero din Divizia Specială au percheziţionat un apartament de două camere din Wood Green Lane (nordul Londrei) şi au descoperit o fabrică de arme chimice.

Otrăvurile şi gazele provoacă spaimă şi panică în rândul populaţiei. În apartament, ofiţerii Diviziei Speciale au găsit ingredientele, echipamentul şi instrucţiunile necesare pentru a prepara, printre alte otrăvuri mortale, ricină, toxină botulinică (care cauzează botulism) şi „otrava cărnii putrezite", care e la fel de oribilă pe cum sună. „Otrava cărnii putrezite" este considerată de o mie de ori mai puternică decât gazele neuroparalitice şi e nevoie de doar o cantitate infimă ca să provoace moarte instantanee. Presupusa experienţă a lui Bourgass cu otrăvurile a fost subliniată şi de descoperirea unor reţete de preparare a otrăvii cu nicotină, otrăvii cu cartofi şi a cianurii. Un detectiv a descris-o drept fabricare „artizanală" de bombe care nu necesită decât cunoştinţe elementare de chimie şi în care sunt folosite ingrediente de prăvălie. De fapt, totul dădea impresia de diletantism.

Toate materiile prime erau uşor de obţinut. Pachetele de ingrediente găsite în apartament includeau seminţe de ricin, materia primă pentru ricină, una dintre cele mai uşor de fabricat şi în acelaşi timp una dintre cele mai eficiente otrăvuri, ceea ce o face o resursă ideală pentru terorişti. Poliţia a mai descoperit seminţe de măr şi sâmburi de vişine din care poate fi extrasă cianura. Cianura este o substanţă mortală, folosită în lagărele de exterminare naziste în timpul celui de-al Doilea Război Mondial (deşi este nevoie de cantităţi foarte mari de seminţe de măr şi sâmburi de vişine pentru a se obţine o cantitate letală). Investigatorii au mai găsit acetonă, care este folosită în procesul chimic

de extragere a otrăvii din seminţe, şi echipamente folosite pentru a transforma otrava lichidă în gaz. Otrava cu nicotină a fost descoperită într-un borcan. S-au găsit copii cu instrucţiuni despre folosirea obiectelor casnice de zi cu zi pentru a fabrica explozibili, cum ar fi bombe fumigene sau bombe-bliţ, precum şi detonatoarele care le însoţesc. Diagrame cu circuite potrivite pentru detonatoare şi bombe improvizate, folosite în mod curent de teroriştii din întreaga lume, zăceau de asemenea în apartament. Cele mai multe dintre materiale puteau fi cumpărate prin internet. Au fost găsite şi câteva dintre ustensilele de bază ale unui chimist, cum ar fi pistil şi mojar, măcinător de cafea, mănuşi de cauciuc, hârtie sugativă, termometre, retorte, baloane şi pâlnii.

A devenit curând evident faptul că apartamentul din Wood Green era o fabrică de arme chimice, iar formulele, scrise în arabă, aveau o bază ştiinţifică şi fuseseră fotocopiate la moscheea din Finsbury Park, înainte de a fi distribuite în rândul comunităţii musulmane ostile. Instrucţiunile fuseseră scrise de Bourgass şi erau pline de amprentele lui. Când Mustapha Taleb a fost arestat, Divizia Specială a găsit în posesia lui şi un CD pe care erau ridicate în slăvi beneficiile bombardărilor folosind tehnologia modernă. Pe el erau incluse instrucţiuni despre asamblarea şi montarea dispozitivelor de cronometrare.

Mare parte din ceea ce se ştie despre Bourgass a venit din partea lui Mohamed Meguerba, care a fost arestat de poliţia algeriană curând după ce a fugit din ţară, încălcând condiţiile de cauţiune impuse în Marea Britanie. A fost supus unor interogatorii şi a început curând să furnizeze detalii despre celulele teroriste care operau în Londra şi Manchester, precum şi despre alte activităţi care se desfăşurau în moscheea din Finsbury Park, dând în vileag tot ce ştia despre Al Qaeda. Mărturisirea lui Meguerba şi declaraţia de 27 de pagini, obţinute aproape sigur prin tortură, au fost imediat transmise serviciilor secrete britanice. Le-a spus

anchetatorilor că a făcut parte dintr-o grupare care fabrica arme chimice improvizate şi plănuia atacuri împotriva persoanelor civile, „inclusiv evrei", pe teritoriul britanic. Obiectivul era să răspândească spaima şi panica. A declarat că planurile includeau mânjirea cu lichide şi paste otrăvitoare a maşinilor şi a mânerelor uşilor din nordul Londrei. Meguerba a susţinut că ar fi umplut două borcane cu ricina pe care o fabricase şi că i-ar fi dat otrava unui bărbat pe nume Nadir, din apartamentul din Wood Green Lane. Poliţia care a percheziţionat apartamentul a descoperit planurile, dar nu era nici o urmă de borcane cu ricină.

Dacă aţi clona un terorist musulman, cel mai probabil l-aţi face după chipul şi asemănarea lui Kamel Bourgass. Bourgass venise în Dover din Calais, în remorca unui camion, în ianuarie 2000, şi mersese direct la moscheea din Finsbury Park, unde i s-a spus să ceară azil la Centrul de Imigrări din Croydon. Pentru prima solicitare de azil, din februarie 2000, şi-a dat numele de Nadir Habra şi a declarat că s-a născut în 1973. A dat moscheea ca adresă şi a pretins că nu deţine un paşaport. A fost nevoie de 20 de luni ca aplicaţia lui să fie procesată şi respinsă. Apelul lui împotriva deciziei a fost respins în decembrie 2001. Anticipând rezultatul, Bourgass/Habra nu s-a prezentat la apel, evitând astfel arestarea şi deportarea, şi a dispărut în mijlocul comunităţii musulmane din nordul Londrei.

Ascunzându-se de justiţie pe străzile lăturalnice din Tottenham şi Edmonton, el şi-a schimbat identitatea şi a făcut rost de un paşaport francez fals. Când a fost oprit de poliţişti, în iulie 2002, s-a dat drept Kamel Bourgass, un marocan născut în 1975. Poliţia antitero şi Divizia Specială n-au fost în stare să-l identifice drept Nadir Habra, dar au decis totuşi să-i urmărească pe Bourgass şi tovarăşii săi. Apartamentul din Wood Green Lane a fost descoperit în timpul unei anchete separate asupra unei reţele de fraudă extinse în toată Europa, despre care se credea că strângea fonduri pentru Al Qaeda.

În noiembrie 2002, poliţia a efectuat arestări în întreaga parte de nord a Londrei şi l-a reţinut pe Mouloud Sihali, specializat în a face rost de cazare şi acte de identitate pentru cei în căutare de azil. În apartamentul lui din Ilford au fost găsite cinci paşapoarte false, dintre care unul cu poza unui suspect terorist dat în urmărire. Poliţiştii au găsit şi detaliile unei adrese din Thetford, unde l-au arestat pe David Khalef. Sihali şi Khalef au fost condamnaţi pentru falsificare de paşapoarte, dar nu au fost puşi sub acuzare conform Legii împotriva terorismului. Şi totuşi, în servieta lui Khalef au fost găsite documente în arabă, pe care erau imprimate instrucţiuni despre cum să fabrici otravă şi explozibili. Cercetătorii de la laboratoarele Port Down au testat instrucţiunile pentru otrăvuri şi au confirmat că ar putea fi folosite pentru a produce doze letale de toxine. Descoperirea faptului că în Londra trăiau imigranţi care aveau cunoştinţele şi capacitatea de a produce otrăvuri mortale, ce ar putea fi folosite într-un atac asupra capitalei, a avut un impact major asupra forţelor de securitate, iar suspecţii au fost ţinuţi sub supraveghere, luni de-a rândul, de către MI5. Bourgass, pe cale de a deveni cel mai căutat om din Marea Britanie, a părăsit apartamentul din Wood Green Lane cu câteva ore înainte ca poliţia să percheziţioneze imobilul. Amprente şi fotografii de paşaport ale sale au fost găsite în apartament şi transmise tuturor forţelor de poliţie. Dar poliţia nu avea idee în acel moment unde se află sau, şi mai grav, cine e de fapt. Bourgass a ajuns până în Bournemouth, de unde s-a hotărât să ia cursa de noapte de la Weymouth până în Manchester. Avea nevoie disperată de un paşaport fals, astfel încât s-a îndreptat spre o locuinţă secretă din Crumpsall Lane, o stradă liniştită din partea de nord a oraşului. Aceasta era casa unui libian, Kalid Alwerfeli. Decizia aceasta i-a fost fatală lui Bourgass, deoarece poliţia plănuise deja să percheziţioneze imobilul. Laţul începea să se strângă.

Descoperirea apartamentului din Wood Green Lane a fost în mod evident o lovitură importantă pentru serviciile de securitate. Ea a fost rezultatul urmăririi unui pont primit de MI5 din partea poliției antitero pariziene. Clădirea fusese monitorizată de mult timp, iar bărbații care o foloseau fuseseră filmați și urmăriți. Cu toate acestea, în vreme ce prima razie păruse a fi o lovitură grea dată terorismului din Marea Britanie, operațiunea ulterioară a poliției, cunoscută ca „Operațiunea Salt", a fost un dezastru. La ora patru și jumătate în după-amiaza zilei de 14 ianuarie 2003, apartamentul 4 de la numărul 4 de pe Crumpsall Lane a fost percheziționat de ofițerii Diviziei Speciale, de funcționari de la Imigrări și de o Unitate de Ajutor Tactic (UAT) formată din trei oameni și specializată în pătrunderea în locuințe și securizarea acestora. Sarcina acestei unități era de a pătrunde cu forța în apartament. Se bănuia că principala țintă a acestei razii, Sofiane Mihoubi, a cărui arestare fusese ordonată de către ministrul de interne David Blunkett, ca urmare a unei informații primite de MI5, se afla în apartament. Cel de-al treilea locatar era Khalid Alwerfeli, libianul de 31 de ani care închiriase apartamentul. În noiembrie 2002, lui Alwerfeli i se acordase permisul de ședere pe termen nelimitat pentru a rămâne în Marea Britanie. Era singurul membru al celulei care nu era algerian. Intrase în Anglia în 1999, folosind un fals act francez de identitate.

Razia din Crumpsall Lane a fost plănuită imediat după descoperirea otrăvurilor și a explozibililor din Wood Green Lane. Poliția și funcționarii de la Imigrări implicați habar n-aveau cât de mare era pericolul care-i aștepta. Privind retrospectiv, demersul lor nu poate fi descris decât ca accidental. În procesul de la Old Bailey, Nigel Sweeney a enumerat ceea ce el a numit eufemistic „neajunsurile poliției" în această operațiune, care a implicat 23 de ofițeri. El a declarat în fața instanței: „N-a existat nici o evaluare a riscului, nici un ordin operațional scris, nici o cercetare preliminară a incintei, pentru a determina poziția exactă a

apartamentului, nici o informație asupra persoanelor care se găseau înăuntru și nici măcar dacă Bourgass se afla acolo, nici un instructaj operațional serios înaintea raziei, nici o transparență în ceea ce privește rolul fiecărui ofițer, nici o înțelegere de ansamblu asupra importanței țintelor, nici un echipament de arestare pentru imobilizare, nu au existat comunicări bine planificate sau veste antiglonț". Unicul instructaj operațional a avut loc într-un garaj al secției de poliție Collyhurst, în timp ce se schimbau turele de serviciu. Supravegherea pare să fi fost făcută în grabă, probabil fiindcă nu a existat destul timp ca să fie instalate camerele și analizate riscurile. Colac peste pupăză, între ofițerii Diviziei Speciale implicați în razie și inspectorul-șef care conducea operațiunea exista o oarecare tensiune, iar rețeaua de telefonie mobilă a Diviziei Speciale a cedat în timpul raziei, obligându-i pe ofițeri să-și folosească telefoanele personale. Un nou eșec adăugat pe listă: Mohamed Meguerba, jucător-cheie în această conspirație, a fost arestat, dar eliberat pe cauțiune, putând astfel să fugă în Algeria, unde a fost arestat mai târziu.

Poate părea evident că, atunci când ținta este o celulă teroristă, e nevoie de precauții speciale din partea ofițerilor de poliție implicați și că, înainte de toate, poliția trebuie să se asigure că toată lumea găsită la fața locului este imobilizată cât mai repede. Dar nimeni nu s-a asigurat de toate acestea. Ulterior, polițiștii au declarat că Bourgass părea liniștit și că ei au ținut să nu distrugă eventualele probe de pe mâinile și corpul lui. Poliția le-a ordonat locatarilor să se dezbrace, apoi să-și pună hainele în pungi și le-au dat suspecților să îmbrace salopete albe. Ofițerii Diviziei Speciale nu purtau veste antiglonț și, timp de 90 de minute după ce au intrat în casă, Kamel Bourgass a fost lăsat să stea fără cătușe. Curelele de plastic care se folosesc în mod normal pentru a lega mâinile suspecților rămăseseră la secția de poliție.

Bourgass a declarat un nume fals în fața polițiștilor și a funcționarilor de la Imigrări care au intrat în apartament, însă a fost

recunoscut datorită fotografiilor furnizate de serviciile de securitate. Poliţia ştia că documentele incriminatoare găsite în Wood Green Lane erau pline de amprentele lui Bourgass şi că acesta era un important suspect de terorism. Era evident că el se afla într-o situaţie disperată şi că arestarea lui ar fi echivalat cu ani grei de închisoare, în cazul în care n-ar fi găsit o cale de scăpare. Cu toate acestea, el a fost condus în dormitor de către un poliţist în uniformă pe nume Fleming, care era la prima sa operaţiune teroristă în cadrul UAT. Sofiane Mihoubi se afla în aceeaşi cameră şi stătea pe celălalt pat, unde era păzit de poliţistul Stephen Oake. Aiwerfeli era în camera de zi, sub paza a doi bărbaţi din Divizia Specială. Mai mulţi poliţişti şi ofiţeri de la Imigrări se aflau pe palierul din afara apartamentului, iar alţi câţiva în camera de zi, ocupaţi cu făcutul pozelor şi cu adunatul dovezilor.

Bourgass rămăsese pasiv, neopunând nici o rezistenţă. Aştepta momentul când ar fi simţit atenţia celor care-l păzeau slăbind şi eventual cedând. E genul de bărbat puternic, vânjos, bine clădit, şi avea şansa de a ataca prin surprindere, atuul disperării şi al familiarităţii cu mediul. Era 5.45 p.m. când, fără nici o avertizare, Bourgass s-a ridicat de pe pat, l-a lovit puternic pe poliţistul Fleming în vintre, a fugit în bucătărie, a luat un cuţit cu o lamă de 12 centimetri din suportul de uscare şi a început să înjunghie pe toată lumea din apropiere. „Era gata să ucidă pe oricine i-ar fi stat în cale“, a declarat Nigel Sweeney la proces. În timpul luptei, poliţistul Oake, tatăl a trei copii şi predicator laic în timpul liber, a fost înjunghiat de patru ori în piept. Trei dintre lovituri i-au fost fatale. O lovitură i-a străpuns inima, iar alte două i-au perforat plămânii. Alţi doi ofiţeri ai Diviziei Speciale au fost răniţi în timpul atacului. Unul din ei a fost înjunghiat de două ori în braţ, iar un detectiv al cărui nume nu a fost menţionat, dar care în timpul procesului a fost botezat John, a fost înjunghiat în piept, în lateral şi în spate. Sergentul Paul Grindrod din cadrul UAT a fost înjunghiat în spate şi în

picior. Bourgass a reuşit să nimerească în total 13 lovituri în timpul atacului său turbat.

Consecinţe teribile ale descoperirii unei fabrici teroriste de bombe, pe lângă moartea lui Stephen Oake, au fost şi conştientizarea faptului că serviciile britanice de securitate nu sunt îndeajuns de antrenate sau capabile să facă faţă teroriştilor hotărâţi, nici măcar acelora incompetenţi precum Bourgass. Deşi poliţia şi serviciile de securitate au primit toate informaţiile cu privire la ameninţarea teroristă, acestora le-a lipsit capacitatea să le analizeze şi să le folosească în mod constructiv, astfel încât să-i aresteze rapid şi eficient pe toţi suspecţii. Bourgass era după o încercare nereuşită de a obţine azil, era imigrant ilegal şi, evident, un bărbat instabil şi periculos. Deşi a fost prins, condamnat şi trimis la închisoare, simplul fapt că a petrecut atâţia ani plimbându-se nestingherit prin Marea Britanie şi Europa trebuie să fi fost o încurajare pentru ceilalţi extremişti care erau deja în Marea Britanie. Există dovezi care arată că Bourgass a fost de fapt membru al unei celule teroriste conduse de un algerian, Abu Doha. Se ştie că, în 1998, Doha, cunoscut şi ca „Doctorul“, „Rachid“ sau „Amar Makhulif“, a condus o reţea de asemenea celule. Se crede că a fost membru al „Grupării Salafiste pentru Apel şi Luptă“, care a comis nenumărate atrocităţi în Algeria şi care a fost angajată să organizeze tabăra de antrenament Khalden din Afganistan, unde erau instruiţi membrii nord-africani şi mujahedini. Tabăra pregătea sute de terorişti, iar Osama Bin Laden era un vizitator frecvent, potrivit celor care s-au antrenat acolo şi au fost mai târziu arestaţi. Mulţi dintre ei au fost trimişi să lupte în Cecenia, iar alţii au fost trimişi să lucreze sub acoperire în Occident.

Doha s-a stabilit în nordul Londrei, unde se găseşte o comunitate algeriană puternică, alcătuită din cei care au scăpat de luptele acerbe de la ei din ţară. Potrivit judecătorului Ouseley, care l-a condamnat pe unul din complicii lui Doha, „prezenţa sa, la

fel ca a lui Bourgass, a mărit coeziunea cauzei extremiste algeriene în Marea Britanie“. La sfârşitul anului 2000, în urma unei informaţii primite de la ofiţerii MI6, care au interceptat un apel din partea lui Doha, poliţiştii germani au făcut o razie la o adresă din Frankfurt, unde au descoperit patru bărbaţi, dar şi echipament de fabricat bombe şi o cameră de supraveghere a pieţei Strasbourg. Trei dintre bărbaţii din apartament erau cetăţeni britanici. Toţi au fost arestaţi şi trimişi ulterior la închisoare. Doha, care călătoarea cu un paşaport fals, a fost arestat la Heathrow în februarie 2001, în timp ce încerca să prindă un zbor spre Arabia Saudită. Apartamentul său din Edmonton s-a dovedit a fi o sursă bogată de dovezi acuzatoare, incluzând instrucţiuni de fabricare a bombelor şi paşapoarte false. Doha rămâne în custodie la închisoarea Belmarsh şi se apără pentru a nu fi extrădat în Statele Unite. Nimeni nu pare a şti dacă reţeaua de terorişti a lui Doha îşi continuă activitatea sau dacă s-a dizolvat, odată cu arestarea lui Bourgass. Activiştii din taberele Al Qaeda sunt antrenaţi să se descurce singuri şi să continue, dacă e nevoie, fără alţi membri activi.

Ahmed Ressam, terorist condamnat care se află închis în Statele Unite, după ce a plănuit un atac cu bombă asupra aeroportului din Los Angeles, era în strânsă legătură cu Doha înainte de arestarea sa. Ressam a fost prins în Seattle purtând arme şi explozibili pentru a fi folosiţi în atac. Ameninţat de o condamnare la 130 de ani de închisoare, el a decis să coopereze cu FBI-ul. Djamel Beghal din Leicester, un alt membru al celulei, a fost arestat în Dubai în 2001, sub acuzaţia de plănuire a unui atac asupra Ambasadei Statelor Unite din Paris. El rămâne închis într-o închisoare franceză. Un fost fotbalist profesionist tunisian, Nizar Trabelsi, care s-a antrenat şi el cu Doha în Afganistan, a fost arestat în Bruxelles, având asupra lui echipament pentru fabricarea bombelor; se bănuieşte că el se oferise voluntar pentru un atac sinucigaş cu bombă. Trabelsi

plănuise să bombardeze baza militară aeriană NATO Kleine Brogel. După introducerea în 2001 a Legii puterilor de urgență, mai mulți bărbați suspecți de a fi membri ai rețelei lui Doha au fost reținuți. Noul conducător al rețelei, Kadre, a fost arestat la Londra, în timp ce se îndrepta – după cum bănuiește poliția – către Bourgass, pentru a-l activa și a-i da o mână de ajutor în complotul cu ricină. Bourgass a fost reținut două luni mai târziu, iar arestarea lui marchează probabil sfârșitul acelei celule. Privind retrospectiv, planul de a folosi ricină și „otrava cărnii putrezite" (cu sonorități atât de dezgustătoare) pare excentric, dar el ar fi putut să aibă loc și ar fi creat cu siguranță o panică îngrozitoare în capitală. Ar fi făcut de asemenea să crească tensiunile dintre musulmanii care respectă legea și comunitățile în care ei trăiesc.

Procesul lui Bourgass pune câteva probleme grele MI5-ului și în special Serviciului de Imigrări. De mulți ani, agențiile franceze de spionaj avertizau serviciile secrete britanice că algerieni implicați în atrocitățile din propria țară și nu numai se strecurau în Marea Britanie și cereau azil. Dar nu s-a făcut mai nimic în această privință. Autoritățile britanice și-au justificat inacțiunea spunând că n-au avut nici o dovadă de încălcare a legii. Atacul asupra turnurilor gemene și noua legislație împotriva terorismului au schimbat, după cum era și firesc, toate acestea și au acaparat atenția serviciilor secrete. Din acel moment, serviciilor franceze de spionaj li s-a acordat mai mult credit și se pare că de atunci a fost ținută sub supraveghere comunitatea algeriană. Trebuie totuși precizat că „supravegherea" n-a fost prea satisfăcătoare. În ciuda celor declarate, Bourgass putea să vină și să plece după bunul plac, călătorind în Europa cu acte false și schimbându-și în mod constant identitatea, fără a atrage atenția autorităților. Pretinsa creștere a supravegherii n-a avut un impact prea mare, iar Serviciul de Imigrări a demonstrat o relaxare îngrozitoare. Se pare că se bănuia de mult timp că moscheea din

Finsbury Park ar fi folosită ca adăpost de către imigranţii ilegali şi ca loc de obţinere a documentelor de identitate false, dar a fost pusă sub investigaţie abia atunci când putea fi prea târziu. Algerienii cu care se asociase Bourgass nu au fost opriţi la nici unul dintre porturile sau aeroporturile prin care au trecut. Există aproape o sută de milioane de intrări în Marea Britanie în fiecare an şi, desigur, numai un mic număr e reprezentat de terorişti. Totuşi, există foarte puţini angajaţi disponibili la Imigrări care să verifice cine trece şi să ia măsuri în privinţa vizitatorilor suspecţi. Pare greu de crezut acum, dar în 2002, în Londra nu erau ofiţeri ai Serviciului de Imigrări de serviciu după ora cinci.

Americanii, cu graniţele lor poroase din nord, sud şi est, luptă cu imigraţia la asemenea proporţii cu mult timp înaintea britanicilor. Orice plan care are o şansă cât de mică de a ţine indivizii nedoriţi în afara ţării trebuie să poată asigura paza coastelor sale enorme şi a frontierelor, precum şi a spaţiului său aerian. Atacul de la 11 septembrie a inspirat un apel naţional pentru întărirea securităţii frontierelor şi, cel mai important, a cerut un răspuns la întrebarea: „Cum împiedicăm alte atacuri?" Prima decizie luată, o consecinţă imediată a dezastrului, a fost ca toate aeronavele comerciale care zburau să fie aduse la sol pe cel mai apropiat aeroport, astfel încât inamicul să nu poată folosi văzduhul. Decizia avea sens din punct de vedere operaţional, deoarece, la momentul respectiv, se aflau în aer numeroase aeronave încărcate cu armament militar şi exista un mare risc ca o cursă aeriană nevinovată să fie doborâtă de vreun pilot de luptă mai nervos şi nerăbdător să apese declanşatorul. Dar asta implica şi faptul că tuturor cetăţenilor americani care respectă legea le era interzis să călătorească cu avionul. Să opreşti reţeaua de trafic aerian e ca şi cum ai recunoaşte că nu o poţi apăra, ceea ce face mai mult rău poziţiei ţării decât chiar teroriştii de la care a pornit totul. Numai în 2002 au fost

8 789 123 de decolări civile în Statele Unite – adică o medie de 24 000 de zboruri pe zi. Un total de 539 883 008 pasageri s-au înregistrat în aeroporturile americane în 2002, ajungând la aproape un milion şi jumătate de pasageri în fiecare zi a anului. În Statele Unite, transportul aerian este o industrie enormă şi vitală, bazându-se pe sute de aeroporturi comerciale. E clar că este imposibil să previi orice penetrare a perimetrului aeroportului fără a restricţiona puternic fluxul zilnic al traficului aerian.

Administraţia Bush era perfect conştientă de vulnerabilitatea Statelor Unite la un atac şi de cât de uşor poate fi paralizată reţeaua de transport. Sunt vreo duzină de ţinte care, dacă ar fi atacate şi grav deteriorate, ar lăsa foarte repede naţiunea în impas. De exemplu, râul Mississippi curge din Minnesota până în Golful Mexic şi este, normal, străbătut de un număr mare de poduri. Cel mai încărcat trafic rutier şi feroviar este limitat, totuşi, la vreo 20 de puncte de trecere. Dacă doar şase dintre aceste puncte de trecere ar fi scoase din acţiune, drumul de la est la vest şi traficul feroviar ar suferi întârzieri enorme, iar economia Statelor Unite ar fi paralizată. O problemă asemănătoare există în Manhattan, care, într-o zi obişnuită a săptămânii, are o populaţie lucrătoare de aproape trei milioane de oameni. Există numai şase poduri şi patru tunele ca să ajungi sau să pleci de pe insulă. Un atac chimic sau biologic ar putea lăsa insula izolată, provocând panică în masă; ar cauza întreruperea transmisiunilor TV şi a sistemelor financiare din Statele Unite şi ar putea aduce disperare naţională. Daune grave ar putea fi aduse industriei petroliere chiar şi numai blocând Canalul Naval Houston, de-a lungul căruia petrolul este transportat pe vase din Golful Mexic, pentru a alimenta rafinăriile din Pasadena. O navă-cisternă scufundată ar cauza instantaneu un deficit de petrol în Statele Unite. Din cauza progresului, ţările industriale sunt întotdeauna vulnerabile la atacuri cu bombă în centrale electrice, nave sau clădiri guvernamentale. După distrugerea turnurilor gemene, administraţia

n-a avut ce face altceva decât să avertizeze asupra eventualelor atacuri viitoare şi să solicite o legislaţie dură.

Imediat după atacul asupra turnurilor gemene, serviciile de securitate şi de imigrări au primit sarcina de a crea un nou program de monitorizare a pasagerilor, pentru a preveni repetarea unei asemenea atrocităţi. Identificarea unui număr mic de potenţiali terorişti din cele zece milioane de mişcări zilnice ale pasagerilor necesită munţi de informaţii, din care potenţialii terorişti trebuie identificaţi şi separaţi de majoritatea covârşitoare a oamenilor care nu reprezintă nici un fel de ameninţare la adresa statului. Trebuie creat un program permanent, care să examineze electronic fiecare rezervare a pasagerilor care intră sau ies din aeroporturile americane civile, să identifice călătorii şi să creeze un profil pentru fiecare călător. Anomaliile sau profilurile care nu se încadrează în criteriile stabilite de agenţiile de spionaj ar fi verificate, pentru a se decide dacă indivizii identificaţi aparţin sau nu unei organizaţii teroriste. Acesta este un plan uriaş şi care ar putea avea urmări dezastruoase.

Programul CAPPSII era atât de sensibil şi secret, încât în timpul alegerilor prezidenţiale din 2004 a trebuit să fie abandonat discret şi temporar. Cheia programului o reprezintă implicarea unor companii ca Acxiom Corporation, o companie ce analizează scoringurile de credit şi deţine detalii despre aproape orice persoană din Statele Unite sau Europa. Partenerii săi, NC Software, sunt specializaţi în detectarea riscurilor şi au creat un software pentru analize complexe şi detaliate ale tranzacţiilor comerciale simple. Aceste companii pot procesa simultan miliarde de înregistrări şi au experienţă în lucrul cu industria de asigurări, cu emitenţii de cărţi de credit şi cu companiile de telefonie. Sunt experţi în detectarea fraudelor înainte şi după ce acestea au loc.

O mare parte din industria de procesare a datelor şi-a oferit serviciile gratis agenţiilor americane de impunere a legii încă

de când turnurile gemene fumegau. În doar câteva ore s-au primit cereri de analiză a bazelor de date din partea FBI-ului, a serviciilor secrete şi a poliţiei. LexisNexis, care este uneori confundată cu o agenţie de resurse legale sau de monitorizare a presei, a sărit şi ea imediat în ajutor. LexisNexis este de fapt o subsidiară a editurii-gigant britanice Reed Elsevier, care are sediul în Londra, dar şi subsidiare americane. LexisNexis deţine rapoarte detaliate despre milioane de persoane, familii şi companii, achiziţionate iniţial de la arhivele publice şi conţinând numere de la Protecţia Socială, date de naştere şi multe altele. La început, compania a funcţionat drept bibliotecă legală a Fiscului american şi a creat un sistem de telecomunicaţii pentru a ajuta la o funcţionare mai rapidă a serviciului pe care Fiscul îl pune la dispoziţia clienţilor săi. La sfârşitul anilor 1990, LexisNexis a cumpărat o afacere intitulată Risk-Wise, care evaluează automatneregulile şi potenţialul de risc. LexisNexis putea acum să acorde o „notă“ persoanelor, bazată pe factori precum probabilitatea lor de angajare, experienţa sau nivelul lor de competenţă într-un anumit tip de muncă. Capacităţile companiei LexisNexis erau ideale pentru ca administraţia să încerce să evalueze potenţialul de risc al unui dezastru asemănător cu cel care tocmai lovise Statele Unite.

În prezent, LexisNexis deţine 16 000 de baze de date, are trei milioane de abonaţi şi foloseşte 36 000 de surse de informaţii, cum ar fi arhive publice, decizii ale curţilor judecătoreşti, rezultate financiare, evaluări de credite şi chiar zvonuri. Lucrează pentru serviciile de spionaj, pentru presă şi pentru cei din sistemul judiciar. Când vrei să verifici dacă o persoană e potrivită să lucreze cu copiii, LexisNexis îţi va furniza un portret de ansamblu al aplicantului, incluzând eventuale condamnări penale şi aproape orice altceva te-ar putea interesa. Sistemele companiei procesează şi analizează informaţii despre milioane de persoane, răspunzând la o diversitate de criterii. Ca urmare a haosului de

după dezastrul din New York, LexisNexis a fost de acord să înfiinţeze un grup operativ, „Dezastrul central“ în Washington DC, şi să-şi pună bazele de date la dispoziţia tuturor agenţiilor de impunere a legii. Atmosfera dominantă în acel moment era că ar trebui făcut tot posibilul ca toţi cei vinovaţi de această atrocitate să fie prinşi şi trimişi la puşcărie. Aceasta nu numai din cauza dorinţei de răzbunare, dar şi fiindcă autoritatea şi independenţa Statelor Unite trebuiau apărate cu orice preţ. Nu există nici o limită a cooperării pe care industria comercială era dispusă s-o ofere. Agenţiile furnizoare de date ştiau că ajutorul lor era nu numai vital, dar şi o investiţie în bunăvoinţă care le va aduce profit în viitor. Peste noapte, informaţiile colectate în mod profesionist au devenit un bun nepreţuit. Pentru unii, tragedia de la 11 septembrie a devenit, în mod evident, o oportunitate de afaceri nepreţuită.

Sistemele şi computerele LexisNexis au fost conectate imediat la computerele guvernului şi la bazele de date ale serviciilor de spionaj. Nu e nici o surpriză că una dintre priorităţile companiei era să-şi folosească tehnologia de evaluare a riscurilor ca metodă de analiză a credibilităţii identităţilor date de cetăţenii neamericani care s-au înscris la cursuri ale şcolilor de aviaţie. Administraţia Bush a elaborat o listă cu aproape 20 000 de suspecţi de terorism, având la bază tot felul de criterii îndoielnice, iar LexisNexis a primit sarcina de a-i monitoriza constant. Majoritatea numelor de pe listă nu se făceau vinovate de nici un delict, dar tehnicile companiei au înregistrat câteva succese notabile, identificând, de exemplu, o casă din Florida, pe care teroriştii care deturnau avioane o împărţeau când participau la cursurile de pilotaj.

LexisNexis era conştientă de temerile guvernului american privind faptul că era vorba de o companie britanică, aşa că a depus toate eforturile ca să fondeze în 2003 o nouă subsidiară, denumită LexisNexis Special Service. Lucrul acesta a fost

pe placul avocaţilor guvernamentali, al serviciilor secrete şi al agenţiilor de impunere a legii, dar şi al administraţiei Bush, iar compania a primit imediat permisiunea să lucreze cu cele mai delicate secrete ale Statelor Unite. Noua companie a devenit responsabilă cu Proiectul Securităţii Aviatice, CAPPSII, la care a început să lucreze împreună cu o nouă agenţie guvernamentală, numită Oficiul Naţional de Evaluare a Riscurilor. Din acest moment, LexisNexis a început să ceară bani pentru serviciile oferite.

În 2003, organizaţiilor pentru libertăţi cetăţeneşti au început să le ajungă la urechi zvonuri despre CAPPSII şi despre conceptul de a aplica evaluări ale riscurilor şi ameninţărilor tuturor aeronavelor de transport, pasagerilor, aeroporturilor şi zborurilor efectuate în Statele Unite, precum şi ale fiecărui pasager care zboară în sau din Statele Unite. Un grup denumit Centrul pentru Intimitatea Datelor Electronice (EPIC) a fost foarte deranjat de ceea ce auzea. Acum pare uimitor faptul că Departamentul de Stat şi Departamentul Securităţii Interne au omis să împărtăşească informaţiile despre sistemul CAPPSII grupurilor de presiune ce apără drepturile cetăţeneşti sau mass-mediei, deoarece era un subiect ce nu putea să nu iasă la lumină, iar când acest lucru s-ar fi întâmplat, răspunsul ar fi fost pe măsură. Şi exact asta s-a întâmplat. Guvernul a fost prins punând la cale cel mai amplu sistem de supraveghere internă impus vreodată publicului american, fără să dezvăluie vreun detaliu organizaţiilor ce ar fi fost cele mai interesate de aceste informaţii.

David Sobel, consilier general în cadrul EPIC, s-a opus imediat conceptului ce a ajuns să echivaleze cu nişte „identităţi guvernamentale“ pentru oricine doreşte să călătorească. Alte propuneri au ieşit la iveală curând, cum ar fi folosirea camerelor cu raze X şi a profilurilor finanţate de stat. Sobell şi alţi activişti au protestat pentru simplul motiv că nici o bază de date atât de uriaşă şi de flexibilă precum CAPPSII nu poate fi precisă.

El a argumentat că FBI-ul a admis că baza sa de date privind infracţiunile are un procent de eroare de 33%. Cum sistemul CAPPSII a fost introdus fără ezitare, guvernul Statelor Unite a creat o listă cu persoanele care nu au dreptul să zboare şi a început s-o aplice. Treptat, au apărut poveşti conform cărora tot mai multe persoane respectabile erau oprite la ghişeu, fiindu-le refuzată permisiunea de a se îmbarca. Au existat întotdeauna astfel de liste – atât în Marea Britanie, cât şi în Statele Unite –, însă nici unul dintre indivizii ale căror nume erau transmise birourilor liniilor aeriene sau aeroporturilor din întreaga ţară nu li se spunea de ce erau selecţionate. Lista cu nume furnizată de comunitatea spionilor şi de Departamentul Securităţii Interne părea să crească pe zi ce trecea. Deseori persoanele de pe ea aveau nume arabe sau asiatice, dar rar existau explicaţii suplimentare. Orice tentativă de a pune sub semnul întrebării clasificarea celor care „nu li se permite să zboare“ era imediat respinsă. Şi specialiştii implicaţi în sistemul CAPPSII au devenit curând chiar ei îngrijoraţi cu privire la proiect proiectului, motiv pentru care acesta a fost trecut cu discreţie pe linie moartă în perioada alegerilor prezidenţiale din 2004. Apoi el a fost resuscitat. Simon Davies, reprezentant al grupului de presiune Privacy International, l-a descris ca „un dezastru gata să izbucnească“. El a spus: „Vor apărea erori judiciare şi ştim din experienţele anterioare că va fi un haos la o scară fără precedent în aeroporturile ţării“.

Reprezintă oare CAPPSII viitorul? Singurul mod satisfăcător de a ne stabili adevăratele date de identitate este, în ultimă instanţă, să avem un cip electronic implantat sub piele, cel mai sigur la naştere.

CAPITOLUL X

Cum procedează europenii

Odată cu Războiul din Irak, prăpastia politică dintre Europa şi Statele Unite s-a adâncit considerabil. Francezii nu doar au refuzat să se implice în Războiul din Irak, ci au şi câştigat un imens capital politic de pe urma poziţiei adoptate, iritându-i, în acelaşi timp, pe americani. În ciuda atacurilor cu bombă din 2004, de la căile ferate din Madrid, în Spania vecină, francezii nu par să se teamă prea mult de posibile violenţe teroriste. Dacă vizitaţi Parisul sau Lyonul, o să observaţi că aceste oraşe au şi ele problemele lor legate de criminalitate şi de imigraţie, dar, cu toate acestea, supravegherea publică este cumva mai puţin intruzivă ca în Marea Britanie. Prin contrast, autorităţile britanice au dezvoltat o atitudine dezinhibată faţă de supraveghere, iar Marea Britanie a ajuns acum una dintre cele mai supravegheate ţări din lume. Avem o lungă tradiţie de activităţi teroriste în insulele britanice, iar orice semn care ar sugera o schimbare de comportament al IRA duce rapid la o creştere a supravegherii din partea statului şi a activităţii serviciilor de informaţii. Iar noi tindem să acceptăm această situaţie aproape fără să ne plângem, crezând, poate, că într-o zi problema terorismului va dispărea, iar lumea va reveni la normal.

Dar cum stau vecinii noştri europeni? Ani de zile, olandezii au fost cei mai liberali oameni, totuşi, toate acestea s-au schimbat

când Pim Fortuyn a fost asasinat. Germania a suferit cât s-a aflat în mâinile grupului Bader Meinhof, dar ţara a părut să aibă alte probleme în acea perioadă, iar terorismul era ceva mai jos pe lista preocupărilor. Deci, ce se întâmplă cu Europa?

Odată cu Războiul din Irak, sentimentele antiamericane tot mai profunde ale francezilor au părut să întărească nevoia de libertate şi intimitate a ţării, în ciuda conservatorismului său inerent. Nu prea găseşti supraveghere video în Franţa şi Germania, după ce ieşi de pe autostradă. Punctele fierbinţi ale criminalităţii din centrele oraşelor sunt monitorizate câteodată, dar lucrul acesta nu este prea bine văzut şi duce adesea la nelinişti şi demonstraţii. De îndată ce camerele de supraveghere sunt instalate, membrii unui grup de presiune francez numit „Regardez Vous" („Priviţi-vă") apar, invariabil, şi vopsesc cu negru lentilele camerelor. Gruparea a călătorit până şi la New York şi a demonstrat în Times Square. Violenţele puse în practică la McDonald's, în Paris şi în oraşele şi orăşelele de provincie, nu se datorează doar unei percepţii pe care o au unele grupuri franceze cum că acestea ar reprezenta nişte simboluri culturale americane intruzive, ci şi obiceiului acestei companii producătoare de hamburgeri de a instala camere pentru supravegherea clienţilor şi, ocazional, a angajaţilor. Intransigenţa franceză referitoare la Războiul din Irak nu a făcut decât să înrăutăţească lucrurile.

Americanii au decis să intre în forţă în Irak în 2003, presupunând că şi celelalte naţiuni – şi în special aliaţii lor tradiţionali, precum Franţa – vor fi bucuroase să cedeze puţin din autonomia lor naţională, în schimbul prosperităţii şi stabilităţii. America, în calitatea ei de cea mai puternică naţiune a lumii, cerea de la celelalte state o recunoaştere clară a puterii sale şi, de asemenea, un acord tacit cu viziunea Statelor Unite asupra situaţiei politice globale de după sfârşitul Războiului Rece. Greşeala americanilor a fost să presupună că sprijinul automat va veni imediat după decizia de a intra în război împotriva Irakului.

Să alegi a fi aliat cu America era de bun-simț pentru mulți dintre politicienii de ambele părți ale divizatului eșichier politic din Marea Britanie. La urma urmei, puterea militară americană este fantastică, așa încât poate părea o idee bună să beneficiezi de pe urma umbrelei sale protectoare. Și, oricum, pentru mult timp înțelegerea a sunat cam așa: „Ajutați-ne și o să vă ajutăm și noi". Totuși, a existat un alt factor care a cântărit mai greu pentru europeni. Puterea Americii era atât de mare încât, atunci când a venit vorba de politica externă, Statele Unite aveau multe posibilități din care să aleagă, iar acest lucru o făcea să fie o țară imprevizibilă. Nu poți să știi niciodată în ce vei fi târât – și nici măcar dacă Statele Unite nu se vor întoarce într-o zi împotriva ta. Ce-și doreau Franța și Germania era o Americă mai previzibilă și rațională.

Statele Unite nu au realizat că, timp de aproape un deceniu, acțiunile sale au fost percepute ca ostile în țări precum Franța, Germania, Rusia și China. Lumea islamică, în particular, a cam luat bătaie de la Statele Unite în Somalia, Bosnia, Kosovo și Irak. Intervențiile Statelor Unite, împotriva a ceea ce au fost considerate planuri ale Al Qaeda de creare a unui stat islamic transnațional, le-au permis, pur și simplu, grupurilor fundamentaliste musulmane să eticheteze America drept dușmanul islamului și să mobilizeze, astfel, un și mai mare sprijin pentru cauza lor. Al Qaeda s-a născut ca urmare a Operațiunii „Furtună în deșert" – invadarea Irakului în 1990, condusă de Statele Unite –, iar gruparea a prosperat de atunci încoace. Așa încât a existat opoziție la adresa războiului împotriva Irakului – și nu doar dinspre lumea islamică, ci chiar din partea vechilor aliați ai Americii din perioada Războiului Rece.

Francezilor, creșterea puterii americane li s-a părut o amenințare la adresa intereselor economice și strategice ale Franței în Orientul Mijlociu, așa încât readucerea Statelor Unite cu picioarele pe pământ a devenit parte a politicii externe franceze.

Franţa era dedicată ideii unei Europe unite, care să acţioneze pentru a contrabalansa Statele Unite, o Europă controlată împreună de Franţa şi Germania. Opoziţia europeană faţă de America ar fi ajutat Comunitatea Europeană să crească, de la o simplă comunitate economică la o putere politică globală majoră. A existat un reziduu de sentimente antiamericane în Franţa încă de pe vremea Primului Război Mondial. Preşedintele francez Jacques Chirac credea, în 2003, că acest sentiment era împărtăşit şi de alte ţări din Uniunea Europeană. Preşedintele Bush şi-a făcut nişte calcule greşite, aşteptându-se ca Franţa să ezite şi să dezbată, pentru ca, în cele din urmă, să fie de acord să sprijine cauza şi să spună „da“ planurilor de detronare a lui Saddam Hussein şi de instaurare a democraţiei în Irak. CIA a raportat că Franţa era de acord cu credinţa britanicilor şi americanilor, potrivit căreia Irakul avea arme de distrugere în masă şi era pregătit să le folosească. Aşa încât administraţia Bush se aştepta ca Franţa să fie de acord cu poziţia Statelor Unite sau să fie forţată să ia poziţie în faţa Naţiunilor Unite şi să explice de ce ţara era pregătită să tolereze armele de distrugere în masă din mâinile lui Saddam.

Statele Unite nu au reuşit să înţeleagă faptul că Franţa vedea decizia americană de invadare drept şansa ideală de galvanizare a Europei sub conducere franceză. Statele Unite nu au înţeles nici gradul de preocupare a Franţei privind creşterea puterii americane, care devenise ameninţătoare pentru interesele europene şi franceze în Orientul Mijlociu. Statele Unite mai credeau că au un aranjament cu Franţa care ar fi apropiat cele două ţări dacă şi când Irakul ar fi refuzat să permită inspectorilor pe probleme de înarmare ai ONU să intre în ţară, în noiembrie 2002. Cu toate acestea, preşedintele Chirac nu avea nici o intenţie să fie de acord cu acest plan, şi, pe fundalul sondajelor de opinie din întreaga Europă, care în proporţie covârşitoare se împotriveau războiului, s-a străduit să creeze o coaliţie antirăzboi.

În ianuarie, Franţa, Germania şi Rusia au respins, în cor, rezoluţia ONU de autorizare a războiului împotriva Irakului.

Secretarul apărării din Statele Unite, Donald Rumsfeld, a ţinut un discurs prin care a descris Franţa şi Germania drept „vechea Europă“. Suna ca o gafă tactică, dar, de fapt, declaraţia era menită să izoleze Germania şi Franţa de restul Europei, din pricina unei temeri în creştere faţă de o axă franco-germană care ar domina politica externă a Europei. Spre sfârşitul secolului XX, Franţa s-a lansat în construcţia unui sistem de supraveghere prin satelit, ambiţios şi provocator, destinat să adune informaţii de spionaj. Din multe puncte de vedere, el este în linie cu Echelon, programul de supraveghere globală condus de Marea Britanie şi America. Echelon se bazează pe o flotă de sateliţi militari şi staţii de recepţie de pe tot globul şi s-a transformat în cel mai mare proiect mondial de colectare a informaţiilor de spionaj. Acum însă există semne clare că, prin intermediul Franţei şi al sateliţilor săi Helios, ţările europene au un sistem propriu de supraveghere internaţională.

Franţa are trei sateliţi-spion pe orbită, toţi operând în legătură cu o reţea de staţii de recepţie care, împreună, monitorizează, colectează şi transmit sistematic informaţii către Statele Unite şi alte ţări. Se ştie că au fost construite staţii de monitorizare în Guiana Franceză, în oraşul Domme din regiunea Dordogne (sud-vestul Franţei), în Noua Caledonie din Pacificul de Sud şi în Emiratele Arabe Unite. Staţiile franceze de monitorizare din Noua Caledonie şi din Emiratele Arabe Unite sunt utilizate pentru a recepta transmisiunile de la sateliţii din spaţiu şi pentru a acoperi transmisiunile din Asia şi din Orientul Mijlociu. Posturile de receptare din Caraibe sunt folosite pentru a intercepta conversaţiile din Statele Unite.

Nu este un sistem exclusiv militar şi, aşa cum se întâmplă şi cu Echelon, datele obţinute sunt trimise deopotrivă către pieţele comerciale şi militare. Proiectul francez este un prim pas către

o încercare paneuropeană de a concura cu activităţile de spionaj globale ale Statelor Unite. Proiectul francez este operat de către Direcţia Generală de Securitate Externă (DGSE), o agenţie se supraveghere şi spionaj organizată similar cu CIA. DGSE a intrat, de asemenea, într-un acord cu agenţia germană de informaţii externe, Bundesnachrichtendienst (BND), pentru împărtăşirea informaţiilor extrase cu ajutorul programului Helios, în schimbul unei finanţări parţiale a proiectului. Informaţiile comerciale sunt transmise direct către conducătorii companiilor franceze şi germane finanţatoare, dar şi către serviciile secrete franceze. Existenţa unui sistem de supraveghere globală nu a fost niciodată confirmată sau negată oficial de către guvernul francez, deşi existenţa lui este acceptată în general de către publicul francez şi este cunoscută în comunitatea internaţională a spionilor.

Spre deosebire de Echelon şi de staţia americană de receptare din Menwith Hill, a cărei existenţă este, de asemenea, cunoscută în Marea Britanie şi Europa, nu prea există dovezi oficiale că Franţa sau orice altă naţiune europeană ar practica o supraveghere sistematică a comunicaţiilor civile şi militare internaţionale. Acesta este unul din subiectele asupra cărora nu se comentează niciodată. Oficialii britanici care sunt familiarizaţi cu sistemul francez admit, în privat, că acesta există, dar spun că ar fi considerabil mai mic decât Echelon. Ziarul francez *Le Point,* într-un reportaj despre spionajul francez, a citat un oficial guvernamental care ar fi spus că, în vreme ce Echelon interceptează aproximativ 3 milioane de mesaje pe minut, sistemul francez interceptează vreo 2 milioane de mesaje pe lună. Dar adevărul este că nimeni nu ştie nimic sigur, iar Direcţia Generală de Securitate Externă (agenţia însărcinată oficial cu securitatea externă, citată mai sus) face, în mod firesc, economie de ştiri. Ceea ce se ştie este că francezii şi-au actualizat unităţile de spionaj prin satelit de la data acelui raport şi că vor continua să facă acest lucru.

Totuşi, Franţa măcar a recunoscut că dezvoltă un sistem de supraveghere internaţională. François Rouselly, şeful personalului din cadrul Ministerului Apărării francez, a admis că sistemul este utilizat pentru monitorizarea crizelor internaţionale care prezintă interes militar pentru armata franceză, dar şi pentru combaterea terorismului şi prevenirea răspândirii armelor neconvenţionale. Franţa a strâns legăturile pe probleme de spionaj cu vecinii săi (Marea Britanie, Germania, Spania şi Italia). Ar fi fost o nebunie să nu facă acest lucru. DGSE a fost în contact strâns cu MI5 în timpul procesului teroristului algerian Bourgass şi are legături cu unităţile din Poliţia Metropolitană engleză care se ocupă de moravuri şi de traficul de persoane. Franţa este placa turnantă pentru infractorii care călătoresc dinspre Africa spre coastele vestice ale Europei şi dinspre Balcani spre Europa. Adevărul este că Europa devine tot mai mult o unitate de spionaj şi de colectare de informaţii, cu putere şi resurse care rivalizează cu cele ale Statelor Unite.

Interceptarea de comunicaţii de către DGSE nu se află sub incidenţa legilor franceze legate de interceptări, care cere ca indivizii ale căror comunicaţii sunt înregistrate să fie suspecţi de infracţiuni, după cum precizează Comisia Naţională de Control al Interceptărilor de Securitate. Supravegherea franceză are, aproape sigur, obiective mult mai îndrăzneţe. Înregistrarea comunicaţiilor, aşa cum este ea practicată de DGSE, nu trebuie să fie neapărat legată de obiectivul de prevenire a activităţilor infracţionale obişnuite.

Se crede că sistemul francez ar ţinti spre sateliţii de comunicaţii civile Intelsat şi Inmarsat, printre altele. Sateliţii folosiţi în proiectul de supraveghere francez sunt din seria Helios, în interiorul unui program numit Euracom. Totuşi, se pare că sateliţii originali, lansaţi la sfârşitul anilor 1990, încep să-şi arate vârsta şi au o capacitate tehnică de interceptare şi retransmisie comparativ scăzută. Drept urmare, se spune că francezii au

pornit o iniţiativă experimentală numită „Cerise“, pentru interceptarea comunicaţiilor prin satelit. Ei au lansat recent un satelit militar de supraveghere Helios mai eficient, numit 2A. El a fost proiectat şi construit în Franţa, având o putere şi o capacitate mult mai mari decât oricare dintre predecesorii săi.

Ultimul model Helios 2A a fost lansat pe orbită de către racheta europeană Ariane, în 2004. El este primul dintr-o nouă generaţie de sateliţi-spion lansaţi de Franţa. Cântăreşte peste 4 tone şi a fost construit de consorţiul industrial condus de EADS-Astrium. Conform francezilor, 2A este destinat să marcheze începutul unei provocări europene la adresa dominaţiei, din cadrul NATO, a serviciilor de informaţii ale Statelor Unite. Racheta Ariane-5 a decolat de la baza de lansare a Agenţiei Spaţiale Europene (ESA) din Guiana Franceză, pe coasta de nord-est a Americii de Sud. La o oră după decolare, Helios 2A s-a separat de rachetă, apoi şase „microsateliţi“ au fost eliberaţi de rachetă în spaţiu.

Ministrul apărării francez, Michèle Alliot-Marie, spunea: „În Europa, vorbim despre cele patru libertăţi ale Uniunii – fluxul liber de informaţii, dreptul la liberă circulaţie, libertatea bunurilor şi libertatea serviciilor –, dar mai există o a cincea libertate, care este informaţia de spionaj. Naţiunile vor să-şi aroge libertatea de a spiona“. Ea a făcut un apel la o mai mare cooperare europeană în ceea ce priveşte iniţiativele de apărare spaţială. „Cu Helios, forţele militare franceze pot beneficia de capacităţi sporite, de o capacitate de reacţie mai precisă şi mai rapidă. Statutul de putere în spaţiu a devenit esenţial, dacă vrei să exişti pe scena mondială.“ Sateliţii Helios I, dintr-o generaţie mai veche, lansaţi în spaţiu de către rachetele Ariane în 1995 şi 1999, erau, tehnic, mai puţin sofisticaţi – şi urmează să fie înlocuiţi. Locotenent-colonelul Inaky Garcia Brotons, din Forţele Aeriene Franceze, a declarat agenţiei de ştiri Reuters, înainte de lansare: „Acest satelit este indiscutabil mai sofisticat. Sistemul

cu infraroşii ne oferă o detectare mai precisă a activităţilor umane. De exemplu, pe vizibilitate redusă sau noaptea, ne poate spune dacă un convoi de camioane se mişcă sau staţionează, sau dacă un reactor nuclear este operaţional sau nu".

Oficiali din domeniul apărării din Franţa spuneau că, deşi generaţia Helios 2 poate să opereze noaptea, nu poate, totuşi, prelua imagini prin nori groşi. Costul total al programului, care include un al doilea satelit ce va fi lansat în următorii trei ani, a fost de peste două miliarde de euro (2,6 miliarde de dolari), din care Franţa acoperise 95%. Francezii sunt remarcabil de reticenţi în ceea ce priveşte flota lor de sateliţi de supraveghere şi planurile lor de a investi şi mai mult în echipamente de supraveghere militară din spaţiu. În ciuda unui cor tot mai puternic de dezaprobare din partea grupurilor franceze de apărare a drepturilor cetăţeneşti, nu par să existe informaţii credibile privitoare la regularitatea posibilelor interceptări, a ţintelor specifice sau a volumului traficului.

Conform unei dări de seamă apărute în de *Journal Officiel de la République Française,* ziarul care publică zilnic activităţile legislative guvernamentale, există nişte acorduri între agenţiile de spionaj franceze şi germane de împărţire a costurilor supravegherii globale prin satelit. Într-o interpelare adresată biroului premierului, privind operaţiunile de spionaj, Nicolas About, un deputat francez, făcea o declaraţie înfiorătoare: „Salutăm resursele pe care guvernul le-a investit în legea acoperind operaţiuni militare de recrutare în serviciile de securitate şi pentru abilităţile operaţionale dovedite în cadrul programului franco-german de supraveghere prin satelit". Această declaraţie pare să confirme faptul că cele două guverne cooperează, în prezent, în chestiunea sateliţilor militari, care pot să spioneze atât populaţia Franţei, cât şi extremiştii islamici din Algeria. Sateliţii Helios sunt folosiţi în misiuni de recunoaştere fotografice, iar datele obţinute din supraveghere sunt împărtăşite agenţiilor de informaţii din Germania, Spania şi Italia.

Există constrângeri financiare evidente pentru acest tip de tehnologie, dar acesta nu este singurul motiv pentru a investi în acest tip de program şi a-l extinde, implicându-i pe aliaţii europeni. Implicarea financiară germană în acest sistem ne ajută să înţelegem de ce administraţia Bush nu a reuşit, în ciuda unor eforturi susţinute, să convingă Bonnul să respingă sateliţii militari francezi şi să accepte ajutorul Statelor Unite pentru a construi capacităţi germane de adunare de informaţii. Francezii au investit recent în patru sisteme AWACS E-3 (Sisteme de Avertizare şi Control Aeropurtate). Sistemul AWACS a fost selectat ca fiind cel care îndeplineşte cerinţele iniţiale referitoare la avertizările aeropurtate ale Republicii Franceze. Această navă reprezintă standardul mondial pentru sistemele de avertizare aeropurtată timpurie; E-3 a fost proiectat şi livrat de către Boeing, iar cele patru E-3-uri ale Forţelor Aeriene Franceze îndeplinesc atât funcţii de supraveghere aeriană, cât şi funcţii de comandă şi control. Le-au fost adăugate funcţii de îmbunătăţire a supravegherii, pentru a îndeplini standardele franceze unice pentru misiuni şi au o capacitate foarte mare de interceptare şi transmitere a semnalelor de la sol sau de la sateliţi. Ele folosesc un sistem de realimentare prin sondă, pentru a creşte receptaculul existent de alimentare în timpul zborului, un înregistrator digital pentru misiunile audio şi echipamente radio îmbunătăţite. Conform unei surse RAF, sistemul francez ESM de avertizare timpurie şi de supraveghere AWACS este un sistem pasiv de ascultare şi de detecţie care permite lui AWACS să detecteze, identifice şi urmărească electronic transmisiile unor surse de la sol, din aer sau maritime. Folosind sistemul ESM, operatorii misiunilor pot identifica tipul radarului sau al armelor. Un element major de sprijin direct îl reprezintă instalaţia franceză a echipamentului misiunii E-3. Boeing a livrat o navă goală pe aeroportul Le Bourget, de lângă Paris, acolo unde au fost instalate sistemele franceze.

Un fapt inevitabil este acela că, în Europa şi în Statele Unite, atât guvernul, cât şi industria sunt de acord că „spionajul prietenos“, din raţiuni politice şi economice, este răspândit printre aliaţii occidentali. Cu alte cuvinte, supravegherea, spionajul industrial, furtul de secrete şi trasul cu urechea, deşi nu sunt acceptabile într-o societate civilizată, sunt folosite oricum. Raportul anual al STOA (Evaluarea Opţiunilor Ştiinţifice şi Tehnologice), organism al Parlamentului European, detaliază operaţiunile de supraveghere ale Statelor Unite; cu toate acestea, Statele Unite au fost scandalizate la gândul că spaţiul le este invadat, iar reţelele de comunicare le sunt spionate. Statele Unite acuză naţiunile europene, precum şi alte ţări, de „spionaj şi colectare globală de informaţii“, incluzând şi operaţiuni de ascultare a cetăţenilor şi a companiilor americane.

Centrul Naţional pentru Contrainteligenţă (NACIC) al Statelor Unite, afirmă, în raportul său anual, că „guvernele străine care conduc activităţi de spionaj industrial“ reprezintă o preocupare reală şi majoră şi, cu toate acestea, nu a fost nominalizată nici o ţară anume. „O serie de ţări străine ridică ameninţări la diferite niveluri şi de diferite tipuri, pentru informaţiile economice şi tehnologice ale Statelor Unite. Majoritatea acestor ţări sunt fie aliaţi pe termen lung ai Statelor Unite, fie ţări neutre în mod tradiţional. Ele au început să ţintească şi să captureze informaţii economice şi tehnologice din Statele Unite, în ciuda relaţiei lor prietenoase cu Statele Unite.“

Franţa este, fără îndoială, una din cele mai active ţări din lume în direcţia adunării de informaţii – şi se consideră a fi în fruntea Europei, când vine vorba de demonstrarea puterii europene. Furtul de informaţii industriale şi economice nu este, de obicei, aşa de sofisticat precum mulţi dintre noi s-ar aştepta şi există o largă paletă de posibilităţi pentru cei implicaţi în adunarea de informaţii care i-ar aduce avantaje în afaceri. De exemplu, domeniul telecomunicaţiilor este ţintit şi interceptat în

mod direct. Cea mai lucrativă dintre toate posibilităţile, neglijenţa referitoare la codarea secretă (criptare) a datelor din sectorul privat, lucru care face posibilă obţinerea lejeră de mari cantităţi de date. Francezii admit că aceste tehnici le oferă cea mai mare parte din informaţiile economice şi industriale obţinute de la corporaţiile americane.

Firmele de telecomunicaţii deţinute de stat reprezintă o altă ţintă pentru supravegherea şi spionajul de stat, iar transmisiile de date vrac din computere şi din poşta electronică şi traficul de faxuri reprezintă o ţintă prioritară, deoarece sunt uşor de accesat şi interceptat. Telecomunicaţiile corporatiste şi în special telecomunicaţiile internaţionale reprezintă, de asemenea, o sursă de informaţii, foarte vulnerabilă şi eficientă, potrivit unor surse neoficiale din cadrul NACIC.

Comunitatea agenţiilor de informaţii ale Statelor Unite acuză deseori naţiunile străine care practică spionajul economic în detrimentul firmelor din Statele Unite. FBI-ul nominalizează Franţa, Germania, Israelul, China, Rusia şi Coreea de Sud în mod constant printre culpabili. Această dezvăluire, evidentă şi, în general, lipsită de necesitate, a Biroului, a fost făcută de Edwin Fraumann, un agent FBI de la sediul din New York, care a redactat o analiză academică asupra spionajului comercial internaţional, publicată de Societatea Americană a Administraţiei Publice, în *Public Administration Review*. Fraumann a pretins că agenţii francezi îi interceptau până şi pe oamenii de afaceri americani care zburau cu avioanele companiei naţionale Air France, precum şi convorbirile telefonice şi comunicaţiile prin fax din hotelurile franceze. Analiza continua şi acuza Germania că operează un post de supraveghere în apropiere de Frankfurt, de unde se monitorizează convorbirile telefonice din Statele Unite şi că încearcă să penetreze sistemele de computere americane. Comparativ cu Echelon, bineînţeles, asta nu e mare lucru. Dar nu prea există îndoială: aceste

înregistrări și monitorizări ale unui grup select de vizitatori, în special din America, sunt constante și profesioniste.

Și cu siguranță că nu există nici o îndoială că Echelon colectează cantități imense de date confidențiale despre afacerile europene. Indignarea Americii este, în consecință, deplasată și exprimată doar ca parte a unui proces de propagandă. Bernd Schmidbauer, directorul serviciilor secrete germane, a negat acuzațiile într-un articol și a declarat că spionajul străin împotriva firmelor germane reprezintă o problemă serioasă și costisitoare. Ca reacție, Franța și Parlamentul European au criticat operațiunile globale de supraveghere ale Statelor Unite și s-au arătat reticente în a coopera în operațiuni de spionaj transfrontalier cu America, din cauza riscului de a atrage o limitare a dreptului la viață privată a cetățenilor și de a încuraja spionajul împotriva companiilor europene. Oficiali ai guvernului francez au confirmat că țara a decis să-și schimbe politica de criptografie în ianuarie 1999, iar acum încurajează utilizarea criptării, din cauza gradului de sofisticare a capacităților de interceptare ale Statelor Unite. Ministrul afacerilor externe francez, Hubert Vedrine, spunea în noiembrie 1998 că, pentru guvernul francez, a devenit o „preocupare" contrabalansarea amenințării reprezentate de Echelon. De fapt, atât Franța, cât și Statele Unite s-au suspectat una pe cealaltă în probleme de spionaj, iar o escaladare a acestei situații datează din perioada Războiului Rece, când Franța a creat politica de reconciliere cu URSS-ul, numită „A Treia Cale". La începutul anilor 1990, Franța a respins inițiativa FBI-ului de cooperare pentru crearea unei baze de date internaționale referitoare la teroriști, pur și simplu pentru că programul era condus de Statele Unite.

„Spionajul prietenos" este un eufemism pentru comportamente de natură să ridice temperatura relațiilor diplomatice. Au fost raportate multe incidente de spionaj comercial și diplomatic între țările occidentale prietene, lucru care a dus la tensiuni

între Europa şi Statele Unite. În decembrie 1995, cinci angajaţi ai Ambasadei Statelor Unite au fost expulzaţi din Franţa după ce au fost acuzaţi a fi agenţi CIA. A fost un incident public straniu, cu implicaţii politice profunde, care a survenit în timpul campaniei electorale pentru prezidenţialele din Franţa şi care l-a făcut pe un agent de informaţii din Statele Unite să declare (către *The Washington Post)* că va dăuna cooperării americano-franceze pe probleme de spionaj pentru mulţi ani de-atunci încolo. Nu fusese nimic altceva decât un gest politic tipic francez destinat să adune voturi. Dar americanii nu au uitat niciodată. Ca o altă ripostă la criticile SUA la adresa Europei, un cetăţean american a fost deportat din Germania, în martie 1997, pentru încercarea de mituire a unui oficial din Ministerul Economiei.

Cooperarea cu Statele Unite, în Europa, nu este neapărat o politică bună, din cauza tensiunilor interne create inevitabil de către acuzaţiile lansate de iniţiativele americano-europene de supraveghere reunită. Mulţi membri ai Parlamentului European şi oficiali ai Comisiei Europene sunt reticenţi când e vorba să accepte orice tip de acord de cooperare pentru activităţile de interceptare ale poliţiilor europene. Motivul este acela că mulţi politicieni europeni văd asta drept încă o cale de întărire a relaţiilor cu FBI-ul şi cu CIA-ul. S-a afirmat că „Rezoluţia asupra Interceptării Telecomunicaţiilor în Contextul Noilor Tehnologii" a Consiliului de Miniştri al UE ar fi fost schiţată cu ajutorul FBI-ului, iar grupul de luptă pentru drepturi cetăţeneşti Statewatch, cu sediul în Marea Britanie, prezentat un document care părea a fi un document de lucru confidenţial al Consiliului, care afirma că FBI-ul participase la schiţarea rezoluţiei în calitate de „grup de experţi" pentru cerinţele tehnice ale interceptării.

Nimeni nu pare pregătit să confirme faptul că Rezoluţia Consiliului pe Probleme de Interceptare Poliţienească (ENFOPOL 98) a avut ca scop doar aplicarea legii sau s-a dorit ca ea să abiliteze o interceptare globală a comunicaţiilor. În Europa s-au făcut apeluri

la cooperarea serviciilor secrete din interiorul Comunităţii Europene, şi, mai exact, într-un document de lucru al Uniunii Europene Occidentale, alianţa militară a Europei, intitulat „O politică europeană a serviciilor secrete“. Un astfel de program ar presupune o colectare de informaţii din zone aflate în afara celor privite de obicei ca preocupări tradiţionale legate de securitatea naţională. Este evident că, dacă UE prosperă şi se consacră ca o putere militară mondială, atunci trebuie să aibă şi capacitatea de a sprijini acest lucru prin activităţile serviciilor de informaţii. Aceste activităţi s-au schimbat serios în ultimii ani. Au fost dintotdeauna o chestiune militară, care depindea, într-o mare măsură, de spionajul uman („Humint“) drept sursă. Deşi sunt încă de uz militar, activităţile serviciilor moderne de informaţii au aproape întotdeauna şi o latură politică, comercială sau religioasă.

Toate guvernele europene sunt cu ochii pe unităţile de supraveghere ale Statelor Unite, stare de spirit care face, în mod firesc, ca orice cooperare transatlantică în domeniul informaţiilor să fie dificil de realizat. În vreme ce Marea Britanie a cooperat total cu Statele Unite în timpul Războiului din Irak şi după acesta, supravegherea a devenit, în Europa, o chestiune pur europeană – şi continuă să fie astfel. Unitatea politică şi economică întărită prin crearea unei monede unice ar putea fi extinsă şi spre alte zone, cum ar fi o abordare europeană conjugată a tehnologiilor de supraveghere, pe care Franţa încearcă, fără îndoială, să o conducă.

Drept urmare, în locul creării unui sistem unic de supraveghere globală a Europei şi Statelor Unite, dacă Franţa şi Germania îşi vor face voia, Europa va ajunge în cele din urmă să-şi realizeze propriul proiect independent, care să-l concureze pe cel al Statelor Unite. O reţea paneuropeană independentă, de spionare şi supraveghere, nu îi va face pe adepţii dreptului la viaţă intimă să doarmă mai liniştiţi în paturile lor, la gândul că drepturile cetăţeneşti le sunt protejate. Ce se va întâmpla însă

va fi că lumea se va trezi cu două sisteme puternice şi intruzive de supraveghere, în loc de unul.

Este evident că Franţa are acum resursele tehnologice necesare pentru supravegherea globală şi că le foloseşte. Iar aceasta ar putea servi drept început pentru o iniţiativă europeană de colectare a informaţiilor, ceea ce va însemna, probabil, că adunarea de informaţii există şi în afara unor legi naţionale consacrate, destinate să protejeze viaţa privată. Şi în arena politică, şi în cea comercială, Europa şi-a întărit securitatea informaţională, prin intermediul tehnologiilor de criptare şi de monitorizare electronică, pentru a se proteja de posibilele interceptări ale comunicaţiilor din partea Statelor Unite. Motivaţia Europei de a investi în tehnologie de supraveghere şi de a dezvolta astfel de tehnologii este, evident, aceea de a contrabalansa cunoştinţele tehnologice ale Statelor Unite. O dificultate majoră este aceea că Statele Unite, în lupta împotriva ameninţării globale a terorismului, solicită acces imediat la informaţiile referitoare la terorişti. Nu este în interesul nici unei ţări să refuze accesul la aceste informaţii, ceea ce înseamnă că relaţiile între Statele Unite şi fiecare ţară din Europa, la nivel operaţional, trebuie să continue să existe. De exemplu, după atacul cu bombă de la Madrid, din martie 2004, noi dovezi ale modului în care teroriştii islamişti au reuşit să nu fie detectaţi, prin aceea că au operat în reţele slab conectate, au apărut ca urmare a unei investigaţii realizate de agenţii de spionaj din Paris şi Madrid. La 11 zile după atrocităţile din capitala Spaniei, descoperirea legăturilor politice dintre un suspect principal în atacul cu bombă şi militanţii islamişti de peste tot din Europa şi din Africa de Nord a făcut dovada creşterii numărului de reţele teroriste cu puţine legături directe cu Al Qaeda, dar cu intenţii similare. Atacul a dezvăluit o „acumulare de straturi din diferite reţele care fuseseră slăbite, dar care au reuşit să fuzioneze şi să se regenereze", după cum spunea Jean-Charles

Brisard, fost agent al unui serviciu secret francez, care a investigat Al Qaeda pentru avocații care au reprezentat familiile victimelor din 11 septembrie.

„Regenerarea unor grupări teroriste ilustrează modul în care amenințarea terorismului s-a mutat dinspre Al Qaeda spre niște organizații asociate, inspirate de Bin Laden, dar care, nu așteaptă neapărat ordine de la acesta", spunea doctorul Rohan Gunaratna, care a scris cartea *În interiorul Al Qaeda: Rețeaua globală a terorii*. „Acest lucru arată că Al Qaeda a devenit o mișcare și nu mai este un singur grup." De câte ori se întâmplă o atrocitate, oriunde în lume, Statele Unite află mai multe despre inamicul pe care și-a propus să-l urmărească fără remușcări. Cheia, spune doctorul Gunaratna, este o cooperare internațională strânsă a serviciilor de informații. „Serviciile de securitate europene încă mai privesc rețelele de teroriști ca pe niște probleme naționale", afirmă el. „Ele nu au ajuns la nivelul de integrare pe care l-a atins Al Qaeda, în ceea ce privește combinarea rețelelor." Totuși, Statele Unite l-au atins.

Desigur, există grupuri de apărare a drepturilor cetățenești care văd pretutindeni conspirații hotărâte să ne deposedeze de dreptul la intimitate, mai ales când vine vorba de cooperarea dintre comunitatea de spionaj americană și Europa. E de înțeles de ce asta face pe toată lumea nervoasă. Drepturile cetățenești reprezintă foarte mult în Paris și Bonn, iar Parlamentul European vede cu ochi răi incursiunile în Europa ale unor agenții de spionaj externe, precum FBI și CIA. Cererile frecvente și mereu respinse venite de la Bruxelles despre ce se întâmplă la Menwith Hill nu sunt de folos. E de înțeles faptul că Franța și Germania doresc să aibă propriile capacități în această zonă.

Distanțarea de Statele Unite în probleme de spionaj vine împreună cu o tendință către cooperare interguvernamentală în domeniul impunerii legii, manifestată de exemplu prin eforturile celor mai bogate țări din lume (Grupul celor Opt și Grupul

de la Lyon) de a combate infracţiunile high-tech sau prin acordul de la Wassenaar privind controlul exportului de tehnologie pentru criptare.

În timp ce aceste discuţii internaţionale continuă, activităţile de supraveghere orientate împotriva cetăţenilor şi companiilor unor naţiuni aliate, cu scopuri diferite de tradiţionala securitate naţională, continuă şi ele. Guvernul german a aprobat o lege de spionaj menită a înlesni autorităţilor posibilitatea de a trage cu urechea la comunicaţiile prin telefoane fixe sau mobile, e-mail, fax şi SMS (serviciul de mesaje scurte). Noua lege le cere furnizorilor de reţele să instaleze şi să menţină echipament şi proceduri care oferă acces la traficul electronic al clienţilor lor, odată ce autorităţile au obţinut un ordin legal de supraveghere. Trasul cu urechea „în cazul suspiciunii de anumite infracţiuni grave" este, se pare, deja permis în legislaţia existentă.

Legea nu se aplică în cazul companiilor private de telefonie, iar cerinţele tehnice sunt limitate la furnizorii de „sisteme de telecomunicaţii publice", care includ operatori de telefonie la sol şi mobilă sau furnizori de conturi e-mail, dar nu şi furnizori de servicii internet. Operatorilor unor modalităţi de transmisie care oferă utilizatorilor acces imediat la internet, cum sunt conexiunile DSL (linie de abonament digital), li se cere de asemenea să-şi instaleze tehnologia de interceptare. În Germania, cel mai mare astfel de operator este Deutsche Telekom AG, fostul furnizor obligatoriu de telefonie, care este încă deţinut majoritar de stat. Guvernul german afirmă că propuneri privind interceptarea convorbirilor au existat dinainte de 9/11, dar au fost aspru criticate de industriile IT şi de telecomunicaţii, care s-au plâns cu privire la costurile mari ale instalării tehnologiei necesare. Desigur, 11 septembrie a schimbat situaţia şi industria a acceptat, în cele din urmă, o soluţie de compromis.

Normal, nu toate temerile industriale au fost satisfăcute de noua lege, potrivit asociaţiei profesionale IT BITKOM (Bundesverband

Informationswirtschaft, Telekommunikation und neue Medien eV); dar legislația în vigoare oferă aparent un compromis acceptabil între interesele statului de supraveghere a telecomunicațiilor și utilizarea neîngrădită a internetului. Planul original ar fi implicat supravegherea angro a furnizorilor de servicii, însă compromisul acceptat de guvernul german pune accentul pe conexiunile utilizator-rețea, ceea ce, afirmă industria, face viața mai ușoară pentru furnizorii de rețele mai mici și de servicii internet.

Bineînțeles, organizațiile de drepturi cetățenești nu au fost potolite prea ușor. 12 grupuri de apărători ai drepturilor omului au compus o declarație comună, avertizând asupra pericolului unui „stat supraveghetor" și menționând experiențele totalitariste ale țării, precum nazismul și comunismul est-german. „Balanța dintre libertățile cetățenești garantate de lege și dreptul statului de a le încălca nu trebuie să fie abolită în interesul unei securități naționale abstracte." Grupurile, care sunt puternice și luate în serios în Germania, includ Uniunea Umanistă, Asociația Germană pentru Protecția Datelor și grupul hackerilor, Clubul de Haos al Computerelor. Ele afirmă că se împotrivesc nu doar legii privind interceptarea telecomunicațiilor, ci și altor măsuri de securitate propuse, cum sunt luarea amprentelor, oferirea datelor studenților către poliție sau supravegherea crescândă a străinilor.

Poate fi argumentat că germanii doar aduc protecția cetățenilor lor la același nivel cu celelalte țări. Statele Unite și Marea Britanie permit interceptarea, iar în Franța au fost promulgate legi ce permit „decriptarea, în anumite circumstanțe, a mesajelor criptate transmise prin intermediul internetului". Grupurile de apărare a libertăților cetățenești au replicat: „Aproape toate măsurile propuse se opun unor drepturi de bază. Însă nici una nu oferă mai multă siguranță cetățenilor". Un purtător de cuvânt al guvernului german a spus: „Dacă nu aveți nimic de ascuns, atunci nu aveți de ce să vă faceți griji". Oare unde am mai auzit asta?

Capitolul XI

Nu votați pentru asta

Alegerile generale britanice din 2005 au fost o afacere deosebit de nesatisfăcătoare. Dezbaterile păreau limitate şi banale, fără nici o consistenţă reală. Mass-media părea să se concentreze asupra promisiunilor încălcate şi a imoralităţii campaniei de management. Şi totuşi, a fost desfătarea supremă pentru un om de marketing! Au fost cheltuite sume enorme în cinci sau şase săptămâni de activitate frenetică. Ambele partide importante au avut echipe mari de campanie, pe care presa, cu obsesia ei pentru cultura celebrităţii, s-a străduit să le transforme în subiecte de ziar.

Cea mai mare parte din acţiune s-a desfăşurat în circumscripţiile marginale, unde câţiva alegători „indecişi" deţineau cheia rezultatului general. Majoritatea acestor locuri aparţineau Noilor Laburişti. La începutul campaniei electorale, toate partidele politice importante credeau că lupta va fi câştigată sau pierdută în aceste secţii marginale vitale. Managerii alegerilor, care au fost nevoiţi să-şi înghesuie planurile într-un interval de câteva săptămâni, au fost apoi obligaţi să-i identifice pe alegătorii pe care voiau să-i abordeze şi să-şi concentreze mesajele asupra lor cât mai convingător posibil. Cea mai eficientă metodă pentru a reuşi era prin intermediul publicităţii şi al poştei directe. Aveau mijloacele pentru a-i aborda pe alegători prin telefon, poştă sau contactându-i personal. Dar cum te pui de acord

asupra mesajului pe care vrei să-l transmiţi? Intenţia mesajelor politice este să se adreseze în acelaşi timp persoanelor individuale, familiilor, comunităţilor. Ele răspund preocupărilor legate de mediu, impozitare, imigrare etc. Dar cum pot descoperi echipele de campanie electorală ale unui partid ce anume îl motivează pe un alegător dacă nu ştiu absolut totul despre el sau ea? Problema lor cea mai evidentă, ai putea crede, e că nimeni nu poate şti atât de mult despre un individ. De fapt, nu e chiar adevărat. Cu puţin timp la dispoziţie şi acces la câteva dosare personale, un analist experimentat poate pune cap la cap destul de uşor ce-l motivează pe un individ. Se întâmplă tot timpul.

Alegerile generale din Marea Britanie din 2005 vor rămâne în amintire mai degrabă pentru ceea ce nu s-a discutat decât pentru ceea ce s-a spus. Europa, de exemplu, a fost un subiect uitat; n-a fost menţionat aproape niciodată, şi totuşi viitorul Marii Britanii în Europa, după cum a dovedit-o referendumul pentru noua Constituţie europeană, va fi una dintre cele mai importante probleme politice ale vremurilor moderne. Nimeni din Partidul Conservator n-a sărit la bătaie pentru economie sau cheltuielile de apărare, sau regiunile rurale. Se prea poate ca aceste subiecte să fi apărut ca probleme locale, dar la nivel naţional se pare că s-au delimitat cu grijă câmpurile de bătaie de-a lungul unor linii înguste. A fost o campanie enervantă la culme din multe puncte de vedere. Au apărut discursuri în limbaj de ziar de scandal, iar sloganurile au fost scrise de PR-işti cinici şi experţi în trasul sforilor, şi apoi repetate la infinit. Presa a stors tot ce-a putut despre conflict, analizând, studiind, condamnând şi, în general, epuizând toate posibilităţile. Dar până şi presa a părut să ezite când a venit vorba de alte probleme importante în afară de imigrare, foste dosare, gafe verbale sau voturi. Comentatorii politici, evident disperaţi să găsească ceva nou de spus, au căzut tot mai mult în extreme. În ajunul alegerilor, *Times,* pe vremuri o publicaţie londoneză respectabilă, a

publicat o pagină pe care principalele două titluri spuneau: „Howard îndemnat să rămână şi dacă este înfrânt“ şi „Sprijinul conservatorilor atinge cel mai mic nivel“.

Cunoaşterea în detaliu a trecutului unui politician este de o importanţă esenţială în timpul alegerilor. Jurnalismul ziarelor de scandal trebuie să fie personal. Ca reporter, trebuie să aplici următorul test unei poveşti: răspunde la întrebările „cine, ce, când, unde şi de ce?“ Elementul vital este întotdeauna „cine?“. Dosarele din baza de date Murdoch Press şi Associated Newspapers conţin informaţii despre vieţile şi micile păcate ale celebrităţilor din lumea politică, industrială, show-business sau, pur şi simplu, a celebrităţilor „înnăscute“. Dar marfa importantă e păstrată în biroul şi seiful redactorului executiv. Când a fost redecorat biroul lui Paul Dacre şi a rămas neîncuiat, angajaţii de la *Daily Mail* s-au servit din belşug din secretele lui şi le-au vândut revistei satirice *Private Eye,* unde se mai păstrează încă o selecţie savuroasă. În oarecare măsură, mass-media există ca să afle, să publice şi să comenteze secretele şi, la fel ca serviciile secrete, îşi va croi drum cu microfoane şi intrări prin efracţie oriunde în lume ca să obţină ceea ce-şi doreşte. Bărbaţii şi femeile ale căror nume apar atât de des trebuie să aştepte ca să afle ce se va mai dezvălui despre ele în continuare – şi când. Desigur, dacă şi-au vândut poveştile prin intermediul unui agent, vor şti exact ce şi când se va publica. Chiar şi atunci, ziare rivale vor face dezvăluiri în avanpremieră. Acestea sunt poveşti pe care reporterii lor au reuşit să le încropească din crâmpeie de informaţii şi jumătăţi de adevăr pe care au reuşit să le culeagă în legătură cu subiectul şi cu evenimentul „senzaţional“ în chestiune. Intenţia publicării detaliilor în avanpremieră este minimalizarea impactului „dezvăluirilor în exclusivitate“ ale celorlalte ziare, pentru a-şi proteja vânzările. E greu să controlezi o poveste odată ce are „picioare“.

Când, în timpul campaniei electorale din 2005, l-am întrebat pe redactorul de ştiri de la un ziar naţional de duminică ce-şi

doreşte cel mai mult pe lume, mi-a spus, fără ezitare, că vrea *fotografii cu Sandra Howard goală.* Se referea, normal, la pozele nude făcute în anii 1960, când Sandra Paul, cum se numea atunci, a avut o carieră de succes ca manechin. Se pare că toate manechinele din anii 1960 s-au dezbrăcat în faţa camerei mai devreme sau mai târziu, de obicei pentru David Bailey. În ceea ce-l priveşte pe redactorul de la ziarul de duminică, cineva, undeva, deţinea astfel de poze cu Sandra, iar el le voia. L-am întrebat, în cazul în care existau şi reuşea să le cumpere, dacă le-ar publica în timpul alegerilor. A ezitat şi apoi mi-a răspuns: „Doar să le am ar fi probabil de-ajuns“. Evident, nu avea nici o legătură cu conceptul de „ştire“.

Dintre toate serviciile care strâng informaţii, presa este probabil cea mai lipsită de remuşcări. Ştie lucruri murdare despre toţi cei din lumea politică – şi politicienii o ştiu. În Fleet Street funcţionează o reţea complicată de afaceri şi înţelegeri nescrise. Unele aranjamente sunt bine cunoscute, precum cel dintre prinţul de Wales şi familia lui şi haitele de paparazzi şi urmăritori care nu-i dau pace niciodată. Înţelegerea este ca familia regală să permită „acces limitat în schimbul intimităţii“. Înţelegerea e încălcată adesea din cauza competiţiei disperate din haita de ogari ai ştirilor, dar în general funcţionează.

Dacă pornim de la premisa că redactori puternici ca Paul Dacre ştiu mult mai mult decât sunt dispuse ziarele să dezvăluie, trebuie să ne întrebăm care sunt implicaţiile acestui lucru. De exemplu, Dacre şi angajaţii lui ar putea şti că Lordul „A“, ministru, îşi înşală soţia, dar preferă să n-o dezvăluie în ziar, iar Lordul „A“ ştie că Dacre e la curent, dar nu ştie de ce el păstrează tăcerea. Oare faptul că Dacre are cunoştinţă de acest lucru pune în mod automat presiune asupra Lordului „A“? Oare simplul fapt de a deţine această informaţie constituie o problemă serioasă? Cine ia decizia finală să publice o poveste? Şi, poate chiar mai important, cum ajunge el sau ea să ia această

decizie? În fiecare săptămână, mii de ştiri şi articole sunt „aruncate“ – refuzate la publicare. De obicei asta se întâmplă pentru că sunt pur şi simplu plictisitoare sau nefondate, sau calomnioase. Dar ce se întâmplă cu ceea ce nu se publică, dar se păstrează la dosar? Cine ia decizia să omoare o poveste înainte ca ea să fie lansată?

Acum câţiva ani, înainte de invazia în Irak din 2001, am petrecut aproape o săptămână într-o bază aeriană NATO din Insurlik, Turcia. Era la mijlocul lui decembrie, în cele şase luni dinaintea campaniei electorale, iar aerodromul era aproape de graniţa dintre Turcia şi Kurdistan. Era un loc dezolant şi mizer, departe de zona turistică de pe coasta mediteraneeană, şi era foarte frig. Insurlik, un oraş aflat la aproximativ 16 kilometri de bază, era zonă interzisă pentru piloţi şi pentru personalul de la sol al bazei militare. În parte, era din cauza rău-famatei închisori a datornicilor. Pe vremea aceea, dacă datorai bani în Turcia, stăteai la închisoare până-ţi plăteai datoria. Dacă nu aveai nici un fel de bunuri sau bani, atunci singura ta opţiune era să-ţi pui familia să se prostitueze. Rezultatul era că oraşul devenise un loc periculos şi violent, în special noaptea, iar comandanţii taberei au interzis orice fel de contact cu populaţia autohtonă.

Baza propriu-zisă nu era un loc cu mult mai sigur. Turcii şi kurzii erau în conflict, grupările teroriste kurde, cum e KSA, bombardau şi împuşcau populaţia civilă din Istanbul. Deşi Insurlik era o unitate NATO unde se aflau detaşamente de infanterie şi flotilă aeriană turceşti, americane, britanice şi franceze, baza era în mod evident deţinută de turci, şi în săptămâna dinaintea sosirii mele aceştia instituiseră o oră de stingere pentru tot personalul militar care nu era turc. Patru zile mai târziu, o santinelă turcească a împuşcat şi ucis un soldat american care ieşise să facă jogging la asfinţit, pe pista din perimetrul bazei.

În comparaţie cu americanii, care dormeau în barăci bine construite şi puteau mânca la McDonald's sau puteau face

cumpărături la PX, unde se vindea orice la preţuri de nimic, soldaţii RAF erau în mare măsură rudele sărace ale bazei. Popotele lor erau barăci de lemn şi, în ciuda frigului extrem, erau forţaţi să doarmă în corturi. În fiecare zi, aparate de zbor Tornado britanice, F16 americane şi turceşti şi Mirage franţuzeşti părăseau baza în număr mare, pentru a patrula spaţiul aerian deasupra părţii de nord a Irakului şi pentru a institui zona interzisă de zbor, impusă de Naţiunile Unite. Era o sarcină riscantă şi delicată, iar radarele irakiene urmăreau adesea avioanele NATO pentru a le testa răspunsul.

După ce am petrecut trei sau patru zile în bază, am început să înţeleg că era ceva în neregulă. Relaţiile cu comandantul turc erau „nesatisfăcătoare" în cel mai fericit caz, şi câteodată, fără nici o avertizare, acesta oprea zborurile de la bază, cu excepţia activităţilor flotei turceşti. Turcii erau bine antrenaţi şi utilaţi cu echipamente militare. Avioanele lor F16 americane erau cele mai bune aparate de zbor de atac din lume şi dispuneau de toate resursele necesare, inclusiv bombe ghidate cu laser şi rachete Hellfire aer-sol.

Echipajul aerian RAF era foarte nemulţumit, dar nu din cauza condiţiilor în care erau nevoiţi soldaţii să trăiască, nici a echipamentului cu care trebuiau să lucreze. Cu două zile înainte de data când trebuia să iau avionul Hercules înapoi spre Londra, am descoperit că ceea ce nemulţumea echipajul aerian era ceea ce se întâmpla când turcii limitau zborurile numai la aparatele de zbor turceşti. Un important ofiţer de zbor RAF mi-a spus că turcii începuseră de curând misiuni de zbor la nivel jos în munţii din sudul şi estul oraşului Mosul, de unde bombardau cu napalm satele kurde.

Faptul că avioane NATO, purtând însemnele NATO, bombardau cu napalm aşezări civile era normal să-i deranjeze pe soldaţii britanici, şi baza era cuprinsă de mânie şi nelinişte. Aveau înregistrarea de supraveghere aeriană cu efectele

bombardamentului, iar unii pretindeau chiar că le văzuseră în timpul patrulărilor menite să-l limiteze pe Saddam Hussein la bazele lui aeriene şi să monitorizeze mişcările militare din partea de nord a Irakului. M-am întors la timp la Brize Norton la sfârşitul săptămânii şi mi-am trimis reportajul şi fotografiile la *Mail on Sunday.* Asta se întâmpla în vremurile nu prea îndepărtate când poşta electronică era o raritate – una de care nu dispuneam –, aşa că m-am decis să călătoresc direct la Londra şi să predau totul redacţiei de ştiri. Simţeam că aveam o poveste importantă despre nişte soldaţi britanici foarte nemulţumiţi, despre brutalitatea turcilor şi despre compromiterea misiunilor NATO în partea de nord a Irakului. Aveam declaraţii din partea ofiţerilor RAF şi a piloţilor francezi care sprijineau ceea ce scrisesem.

Povestea a fost primită în tăcere. „Nu este chiar ce voiam de la tine", a fost răspunsul. În cele din urmă mi s-a spus să rescriu tot şi să vin cu un articol despre băieţii noştri, nevoiţi să trăiască în corturi în deşerturile îngheţate din Kurdistan, departe de casă şi familie, tocmai când se apropia Crăciunul. De fapt, nu observasem prea multă nemulţumire în legătură cu corturile şi condiţiile de viaţă, cauza supărării tuturor erau satele bombardate cu napalm. Până la urmă, povestea n-a fost niciodată publicată. Oriunde aş fi dus-o, redactorii reacţionau la fel – o primire rece şi o ridicare din umeri: „Ne pare rău, nu-i pentru noi". Nu înţelegeam de ce, fiindcă simţeam că e o problemă serioasă, care merita publicitate naţională şi internaţională. N-a fost publicată niciodată, cel puţin nu în amănunt. La vremea respectivă am crezut că a fost din cauză că „Napalm şi kurzi" era la polul opus al poveştii plăcute de Crăciun. M-am înşelat. Problemele dintre kurzi şi turci erau preţul pe care trebuia să-l plătească alianţa NATO şi nu era în interesul nimănui ca problema să fie abordată în presă. Dezvăluirile ar fi putut pune în pericol disponibilitatea unor unităţi militare de mare valoare şi compromite capacitatea NATO de a institui

rezoluțiile Națiunilor Unite. Presa a acceptat să se conformeze și asta a fost tot.

De ce decide presa scrisă să omoare în fașă asemenea povești și să ignore un subiect care este evident de interes național? Există un anumit secret politic important, care n-a fost niciodată făcut public în Marea Britanie. El se leagă de sexualitatea unui politician laburist de vază, care deține în prezent o funcție importantă. Politicianul respectiv nu discută niciodată acest subiect și, totuși, fiecare redactor din Fleet Street îl cunoaște. În mod sigur va fi dezvăluit într-o bună zi și va avea repercusiuni semnificative, deoarece este un subiect pe care, în mod normal, ziarele de scandal l-ar înșfăca și l-ar stoarce până când și ultima picătură de potențial a fost extrasă. De asemenea, cititorii britanici vor vrea să știe (din interes public) de ce această poveste a fost ținută secret atâta timp. Când va exploda în sfârșit, politicianul respectiv va riposta într-o manieră demnă și reptilele vor începe să răstoarne pietrele până vor găsi ceea ce caută, dacă nu or avea deja acel lucru. Poate avea sau nu repercusiuni politice pe termen lung. E imposibil să-ți dai seama.

Întrebarea e: ce considerații conving presa să publice sau să respingă poveștile de acest fel? În cazul atrocităților comise de turci în Irak, se presupune că presa a fost convinsă că dezvăluirea acestor fapte n-ar fi în interesul țării și ar compromite anumite politici operaționale și strategice. E greu să susții această părere, astăzi, dar este posibil ca „muștruluiala turcilor“ nu era nerecomandată de către guvern, și după câteva vorbe șoptite din partea unui ministru important, comunitatea din Fleet Street a decis să distrugă povestea. Cea de-a doua poveste a fost și ea suprimată, din cauza unei cereri venite direct de la părțile implicate. Nu e vorba de o problemă de conduită ilicită. Politicianul respectiv a cerut pur și simplu să se păstreze tăcerea și să nu fie făcute publice aspecte ale vieții lui private. Când subiecte importante nu devin știri și nu li se acordă atenție în

presă, aceasta se datorează, de cele mai multe ori, înclinaţiilor politice ale proprietarului şi ale redactorilor săi executivi sau doar unei mici părţi din reţeaua complexă de legături şi promisiuni ce caracterizează relaţiile din lumea ştirilor. Proprietarii şi redactorii lor discută împreună poveştile şi se pun de acord să nu trădeze alţi proprietari.

Alegerile generale din Marea Britanie au fost memorabile nu doar datorită aparentei limitări a direcţiilor politice puse în discuţie, ci şi datorită faptului că, pentru prima oară, partidele politice au organizat campanii electorale ultramoderne, controlate de echipe de manageri profesionale şi foarte agresive. Partidul Laburist şi Conservator au cheltuit împreună milioane de lire sterline pe transformări şi campanii foarte avansate din punct de vedere tehnic, în încercarea de a influenţa cele opt sute de mii de alegători vitali din locurile marginale, care trebuiau convertiţi la cauza partidului dacă voiau să câştige alegerile. Amândouă partidele ştiau că decizia finală urma să fie determinată de bătăliile locale aprige pentru acele locuri marginale şi că acţiunea va avea loc departe de atenţia mass-mediei. Ambele părţi au făcut eforturi susţinute pentru a identifica micile secţiuni de alegători necesare pentru a reuşi. Liderii conservatori şi laburişti au folosit cât mai mult posibil elicopterele, pentru a se deplasa cu viteză în provincie în timpul campaniei electorale. A fost o goană nebună după voturi, atent planificată ca să se desfăşoare rapid, şi epuizantă din punct de vedere fizic. Michael Howard a afirmat că alegătorii care au contat pentru rezultatul final şi care au trebuit convinşi să renunţe la Noul Partid Laburist ca să existe speranţe pentru conservatori au fost în procentaj mai mic de 2%.

O mare parte din bugetul campaniei laburiştilor de 15 milioane de lire sterline a fost cheltuit în această bătălie pentru locurile marginale, purtată în circumscripţiile electorale vitale. Banii au fost alocaţi mai mult pentru goana după alegători decât

pentru publicitate prin afişe şi presă. Centrul Naţional Laburist de Comunicaţii din Newcastle a înregistrat două milioane şi jumătate de apeluri telefonice către alegători în anul care a precedat anunţul alegerilor. Centrul naţional de apeluri al conservatorilor din Coleshill, lângă Coventry (Midlands), îi vâna, bineînţeles, pe aceiaşi alegători. La un moment dat, centrul de apeluri conservator trimitea zilnic un milion de fluturaşi şi dădea un număr la fel de mare de telefoane. Convingerea prin telefon şi poştă directă nu are prea mare valoare în alegerile politice dacă preocupările destinatarilor nu sunt înţelese şi satisfăcute. Dacă unica preocupare a unui alegător o reprezintă ţiganii care s-au mutat pe câmpul din spatele grădinii, nu prea are rost să i se vorbească despre pensii. Cei aproximativ un milion de alegători-ţintă trebuiau studiaţi şi convinşi corespunzător prin scrisori sau apeluri telefonice, în care se explica politica partidului în legătură cu problemele care-i preocupau şi în care era atacată politica partidului rival.

Ambele partide politice au folosit programe „cu captură de date" pentru a crea o bază de date din codurile poştale, fişele de bibliotecă şi bazele de date ale cardurilor de fidelitate. Înaintea alegerilor, conservatorii au pus la punct sistemul VoterVault, pentru a prezice probabilitatea ca un alegător individual să voteze cu ei sau împotriva lor. Au afirmat că programul avea o acurateţe de aproape 75%. Sursa săpăturilor lor a rămas un mister, deşi atât Experian, cât şi LexisNexis au fost implicate în consilierea partidului, şi informaţiile din cea mai mare bază de date naţională de carduri de fidelitate au fost obţinute prin companii de marketing cu date şi folosite în monitorizare. Strategii asemănătoare pentru a ţinti grupuri-cheie în statele sau districtele nehotărâte au fost folosite de campania Bush în alegerile din 2004.

Ambele partide au ţinut mai puţine conferinţe de presă, iar Partidul Laburist în special a evitat ceea ce considera o presă în general ostilă şi a preferat să caute contactul direct cu electoratul.

Singurul autocar electoral a fost folosit de vicepremierul John Prescott. Partidul Laburist, care a ţintit în jur de trei sferturi de milion de alegători-cheie, a izolat cinci mii de votanţi în toate cele 60 de circumscripţii marginale-cheie. Le-au trimis tuturor prin poştă un DVD cu mesaje de la Tony Blair şi de la candidatul laburist local, în care erau discutate subiecte locale. Acest exerciţiu costisitor şi ambiţios a fost urmat de e-mailuri către o sută de alegători, în care li se spunea personal ce făcuse premierul în săptămâna respectivă, inclusiv faptul că fusese la Buckingham Palace să-i ceară reginei să dizolve Parlamentul, pentru a declanşa alegerile. Au mai făcut de asemenea un jurnal video zilnic, care apărea pe site-ul oficial al partidului, unde erau discutate din nou „punctele de maxim şi minim interes“ ale zilei şi era repetat mesajul care spunea că va fi o campanie dură, în care se va lupta pentru fiecare loc. În tot acest timp, echipa condusă de Lynton Crosby, geniul electoral australian, adus ca să creeze şi să se ocupe de campania conservatorilor, furniza presei liste cu ceea ce se pretindea a fi minciunile spuse de Blair publicului britanic.

Campania a fost memorabilă datorită afirmaţiilor şi contrazicerilor făcute în legătură cu cheltuielile. Acestea nu au fost doar transmise personal de către politicieni, ci au fost de asemenea dezvăluite presei prin „scurgeri“ telefonice constante. Laburiştii au angajat o echipă de comunicaţii media pentru a trimite e-mailuri şi a se concentra asupra jurnaliştilor cu articole despre educaţie şi sistemul naţional de sănătate. Materiale de acest gen sunt de obicei destinate scriitorilor de texte politice şi grupurilor politice de „lobby“ – grupul special de jurnalişti politici cu acces privilegiat la politicienii de marcă –, care rareori divulgă cine anume le-a furnizat informaţia. Dar pe măsură ce se desfăşura campania, a devenit evident că ţinta manevrării politice în timpul alegerilor nu mai era presa, ci deveniseră alegătorii-cheie marginali în persoană. Imboldul a venit din partea strategilor laburişti, zdruncinaţi de reacţia publică negativă

manifestată în timpul campaniei. Deși sondajele naționale arătau un avans al laburiștilor, partidul era îngrijorat, deoarece membrii importanți știau că adevărata campanie are loc departe de ochii presei în circumscripțiile marginale.

Unul dintre consilierii principali ai lui Blair a menționat un discurs ținut cu peste trei ani în urmă la Clubul Național de Presă din Australia. Vorbitorul era Lynton Crosby, care a condus Partidul Liberal al lui John Howard spre o victorie spectaculoasă în alegerile generale din Australia și care încerca acum să facă același lucru pentru Michael Howard. Crosby a atras atenția publicului său australian asupra faptului că, în ultimul timp, mulți comentatori din mass-media nu văd mare parte din campania adevărată. „Nu are loc la televizor, la radio și nici măcar în ziare. Activitatea locală pe teren e cea care contează cu adevărat – scrisori către alegători, cărți poștale, publicațiile de știri, propaganda prin telefon, bătutul la uși..."

Politica s-a schimbat mult de la alegerile din 1997, când Partidul Laburist s-a bucurat de poziția sa neobișnuită de câștigător detașat într-o campanie unilaterală și a încurajat poveștile despre profesionalismul ingenios al organizatorilor campaniei, ca de exemplu al magicianului media Peter Mandelson și al secretarului de presă Alastair Campbell, un erou în domeniul relațiilor publice. Strategiile electorale adoptate de laburiști și conservatori în 2005 nu aduceau nimic nou. Cea care a deschis drumul tehnicilor de manipulare folosite de Howard și Blair a fost industria de marketing și PR. Aceste tehnici au fost create pentru a cultiva influența ascunsă asupra presei în favoarea clienților lor din afaceri și partide politice favorabile afacerilor, ca „Noii Laburiști". Colin Byrne, directorul gigantului de consultanță PR Weber Shandwick, fusese unul din principalii consultanți laburiști în probleme de manipulare. Ghidul Electoral Shandwick a atras atenția, încă înainte de a fi anunțată data alegerilor, că „în ciuda opiniei generale, campania din 2005 va

face un efort concentrat pentru a ţinti campania locală mai mult asupra locurilor-cheie marginale decât orice altă campanie media naţională prezidenţială". A fost o schimbare revoluţionară în politica electorală, care a fost îmbrăţişată de ambele partide principale.

Din 2001, o mare parte a ideilor noi a fost importată din Statele Unite şi, într-o măsură mai mică, din Australia. În special „marketingul prin permisiune", folosit de mult timp în afaceri, a fost adoptat acum şi de politică. „Marketingul prin permisiune" presupune folosirea sondajelor, a broşurilor şi a scrisorilor pentru a-i încuraja pe alegători să răspundă direct unei campanii, să obţină, cu alte cuvinte, „permisiunea" alegătorilor individuali de a intra în dialog cu ei. Folosirea în acest fel a contactului direct permite angajaţilor partidului să vorbească despre subiectele de care este interesat în mod deosebit alegătorul individual. Acest sistem a fost folosit în campania electorală din 2005 de toate partidele politice importante. Conservatorii şi laburiştii au investit din belşug într-un software care selecţiona alegătorii în funcţie de caracteristicile sociale, aşa încât expedierile prin poştă şi apelurile telefonice să poată fi adresate direct alegătorilor interesaţi în mod special de problema respectivă. În teorie, asta înseamnă că, de exemplu, proprietarii de case pot fi destinatarii mesajelor despre subiecte care îi privesc direct, ca ipoteci şi taxa de timbru. VoterVault, aşa cum a fost folosit de conservatori, a fost modelat după modelul american, în timp ce laburiştii au folosit Labour Contact, un pachet asemănător.

Nimic din toate acestea nu e vizibil pentru publicul larg sau presă. La începutul campaniei electorale, când site-ul partidului a lansat un zvon despre posibilele campanii publicitare ale partidului, Alastair Campbell a fost văzut intrând în sediul Partidului Laburist, gata să se alăture campaniei. Una dintre temele următoare îl arătau pe Howard în pielea personajului Fagin al lui Charles Dickens, iar ziarele a luat-o razna condamnând

antisemitismul imaginii. Rezultatul, după cum fusese bineînţeles prezis de Campbell, a fost că povestea a fost continuată la nesfârşit şi le-a dat laburiştilor material din belşug. Partidul a publicat negări ample că ar fi avut motive ascunse, întărind în acelaşi timp afirmaţia că Partidul Conservator devenea zgârcit când era vorba de finanţarea sistemului naţional de sănătate. Scoaterea în evidenţă a originilor evreieşti ale lui Howard şi imaginea lui hipnotizând alegătorii cu un ceas de buzunar cu lanţ s-a întipărit în minte. A fost o tactică abilă, deşi nu putea fi folosită decât o singură dată. Conservatorii nu puteau pune punct poveştii, deoarece nu deţineau controlul asupra ei. Lui Howard i s-a cerut de sute de ori să comenteze, dar a refuzat.

Cele două partide principale şi-au dezvoltat strategii în jurul „locurilor-cheie", concentrându-şi tot efortul asupra unui număr limitat de circumscripţii care ar fi putut schimba tabăra. Au reuşit să dispună de baze naţionale de telefonie, campanii naţionale prin poştă, organizatori cu normă întreagă şi vizite electorale din partea membrilor importanţi de partid în aceste mici câmpuri de bătălie. În cazul laburiştilor, lista locurilor-cheie a ajuns la urechile presei şi însuma 107 de circumscripţii electorale, toate deţinute de laburişti în 2001. În cele din urmă, numărul a fost micşorat drastic în timpul celor patru săptămâni de campanie oficială. Propaganda din uşă în uşă şi analiza ulterioară a reacţiilor şi preocupărilor alegătorilor, folosirea grupurilor-eşalon şi rapoartele regulate la sediu referitoare la mişcările celorlalte partide au fost introduse în baza de date a partidului şi procesate.

Despre conservatori se ştie că au avut o dezbatere internă la începutul campaniei, provocată de întrebarea dacă să aibă un număr limitat şi „realist" de locuri-ţintă sau o listă mai ambiţioasă de obiective, întocmită pe baza câştigării majorităţii. Liberal-democraţii, care nu au reuşit să concentreze resurse asemănătoare în campania lor, au fost totuşi neîndurători cu selectarea

alegătorilor-ţintă şi au încercat să urmeze o politică de „decapitare“ a conservatorilor – concentrându-se, cu alte cuvinte, asupra membrilor importanţi ai Partidului Conservator care deţineau aşa-zisele locuri accesibile. Până la urmă, nu s-a dovedit o politică de succes. În cei doi ani care au precedat ziua alegerilor, principalele partide au efectuat sondaje de identificare a alegătorilor, campanii de propagandă cu broşuri şi prin expediere directă în zonele de care erau interesaţi. Scopul propagandei electorale nu este neapărat schimbarea opiniei publice – ea este efectuată în aşa fel încât agenţii electorali să poată identifica potenţialii susţinători şi să aprecieze atitudinea locală faţă de politica partidului. Partidele folosesc apoi propaganda şi contactul direct, inclusiv până în ziua alegerilor, pentru a fi siguri că susţinătorii cunoscuţi vor merge să voteze. Alegătorii din circumscripţiile marginale sunt consideraţi nepreţuiţi, iar baza de date ale partidului este actualizată zilnic, pentru ca votanţii să fie constant în atenţie. O astfel de abordare n-ar funcţiona niciodată dacă ai încerca să vinzi termopane în loc de filosofie politică.

VoterVault, Mosaic şi Labour Contact sunt bunuri politice de mare preţ şi vor deveni tot mai importante, pe măsură ce vor creşte în dimensiune. Informaţiile, provenite din diverse surse, sunt introduse imediat ce sunt primite de la sediile celor două partide. În timpul alegerilor din 2005, informaţiile le-au fost donate conservatorilor de către susţinători ai partidului. Rezultatul alegerilor din 2005 a fost decis de propaganda electorală ascunsă şi orientată spre piaţă. Una dintre controversele de durată legate de alegeri – în afară de bine-cunoscutul subiect referitor la Irak – a fost felul în care această campanie ascunsă urma să fie purtată, inclusiv intensificarea utilizării votului prin poştă şi tehnicile folosite, care nu respectau recomandările Comisiei Electorale. Toate acestea au ridicat întrebări legate de manipulare şi fraudă, ce vor trebui clarificate.

Conservatorii și-au asumat în mod sigur un risc în tehnicile lor de propagandă din 2005. Au folosit tacticile lui Crosby, precum „fluierul pentru câini“ – adică marea masă a legătorilor nu va „auzi“ subiectele alese, – ele putând fi ascultate și sprijinite de grupurile-țintă cărora li se adresează. În plus, au lansat atacuri la persoană mai răutăcioase decât orice alt mijloc folosit înainte. Deși partidul nu a reușit să ajungă din nou la putere, conservatorii au reintrat totuși în cursă ca un partid important după înfrângerile dezastruoase din precedentele două alegeri. Totuși, după standardele tradiționale ale „partidului de guvernământ“, a fost în mod clar o campanie murdară și incorectă. Lynton Crosby a fost aplaudat când a ținut un discurs lucrătorilor de la Biroul Central, cu două zile înaintea alegerilor. După încheierea numărătorii, se părea că tacticile lui îi aduseseră pe conservatori din nou pe linia de plutire. Mașinațiunile lui Crosby l-au zdruncinat pe Alastair Campbell, care a întocmit un dosar despre felul în care conservatorii au importat tactici dezonorante din Statele Unite și Australia. Într-o conferință de presă pentru jurnaliștii politici, s-a străduit să dea în vileag „trucurile murdare“ ale conservatorilor, o sarcină dificilă pentru omul care întocmise mistificatorul dosar despre Irak. „Nimeni n-a mai încercat așa ceva în politica britanică“, a afirmat el.

Conservatorii au înțeles că, din punct de vedere tactic, nu se putea prezenta ca o alternativă la guvernare. În schimb, Crosby i-a modelat pe conservatori într-un vehicul, pentru a „trimite un mesaj lui Blair“. Strategia era: „Nu pierdeți timpul cu politici de partid, atacați opoziția“. La venirea lui, pe Crosby l-a îngrijorat lipsa arsenalului tactic al conservatorilor, așa că le-a spus că nu vor reuși să facă în șase luni ceea ce ar fi trebuit să facă în ultimii șase ani. A convins partidul să adopte „Strategia Queensland“, adică să transforme o poziție fără speranță într-un avantaj și să convingă alegătorii că „Nu veți câștiga, așa că votați cu conservatorii ca vot negativ, deoarece nu sunt o alternativă viabilă la

guvernare". Strategia funcţionase în 1995 în Queensland, ţinutul natal al lui Crosby, dar în acest caz şi-a asumat un risc considerabil, ţinând cont că un astfel de stil negativ într-o campanie electorală ar putea convinge oamenii să nu mai voteze deloc.

Cealaltă tactică a sa, „fluierul pentru câini", era o altă metodă pentru a „atrage rasiştii". Enervaţi de succesul Partidului Independenţei din Marea Britanie în alegerile din 2004 pentru Parlamentul European, conservatorii au decis să copieze mesajul acestuia împotriva imigrării, care presupunea o îndepărtare de Convenţia de la Geneva în ceea ce-i priveşte pe refugiaţi, atrăgând astfel muncitorii – destinatarii acestui mesaj. Dar ar fi reuşit ei să depăşească numeric alegătorii burghezi de la oraş care ar fi putut să considere dezagreabilă orice aluzie la politica rasistă? Răspunsul depindea de felul în care s-ar fi achitat conservatorii în circumscripţii ca Putney, pe care l-au şi câştigat. În sfârşit, era bine să concentreze campania atât de mult pe Michael Howard? Howard fusese în trecut unul dintre cei mai antipatizaţi miniştri conservatori, iar schimbarea sa de imagine a fost remarcabilă. Dar nu era prea uşor de caricaturizat ca un vampir din întunecatul trecut conservator?

„Spargeţi-i nasul lui Tony Blair", a spus Brian Sedgemore, vechiul parlamentar laburist care şi-a părăsit partidul în timpul campaniei electorale, din pricina opoziţiei sale faţă de Războiul din Irak. „Ştergeţi-i rânjetul de pe faţă", cereau manipulatorii conservatori. Alegătorii au făcut ambele lucruri, până la un punct, dar Blair a rămas la putere, deşi n-a avut o expresie triumfătoare în discursul său de după victorie. A recunoscut că alegătorii au vrut să pedepsească guvernul. A menţionat chiar şi Războiul din Irak şi a recunoscut că a dus la diviziuni, adăugând că speră că ţara va fi unită din nou. Venind la sfârşitul unei campanii în care fusese caracterizat ca mincinos, un pericol pentru propriul partid, o pradă uşoară, şi în care fusese păcălit de un jurnalist să discute despre viaţa sa sexuală, se ridica

întrebarea: Poate Blair să revină? A promis să se retragă în timpul acestui mandat, lăsând puterea în mâinile ministrului de finanțe, Gordon Brown.

Sunt multe modalități de a interpreta aceste alegeri derutante și meschine. Între 1979 și 1992, Partidul Laburist a pierdut patru alegeri la rând, și se părea că nu va fi niciodată ales. Până astăzi a reușit să contureze o nouă democrație socială britanică. În același timp, procentajul său de 36% din voturi populare este „cel mai mic de când Marea Britanie a devenit o democrație", potrivit analistului politic Anthony King. În plus, nu este clar ce idei a lăsat în urmă Partidul Laburist. Promisiunea lui Blair din campania din 2001 de a face serviciile publice să răspundă cererii pieței, permițând oamenilor să-și aleagă singuri spitalele și școlile pe care le folosesc, a fost în mare parte amânată de concentrarea atenției asupra Irakului. De data aceasta, campania Noilor Laburiști semăna mai mult cu „vechiul" Partid Laburist, o promisiune nu de a face reforme, ci de a apăra serviciile de atacurile conservatorilor – „dacă țineți le asta, votați-ne". Însă aceste trucuri murdare de analiză și marketing practicate de ambele părți sunt ceea ce va rămâne în memorie din alegerile electorale din 2005. Dar dacă ar dezvălui cineva toate informațiile secrete din dosarele ce se găsesc la Northcliff House? Ar fi ca și cum s-ar deschide cutia Pandorei...

Concluzii

Trăim vremuri periculoase. Suntem încă implicaţi într-un conflict major în Irak, unde un „război sfânt" între islam şi America creştină continuă să facă victime. În Bagdad, infirmierele de la Centrul de Tratament al Victimelor Torturii continuă să îngrijească irakieni ai căror torţionari nu mai sunt serviciile secrete ale lui Saddam, ci procurorii trimişi de CIA. Nu există încă o strategie de retragere a trupelor americane şi britanice, iar preşedintele Bush încă zdrăngăne din spadă şi ameninţă că va bombarda instalaţiile nucleare din Iran. Cum s-a ajuns la asta? De ce au devenit liderii noştri atât de convinşi că reprezintă forţele binelui în lupta cu un imperiu al răului? De ce vor să ne priveze de intimitatea noastră, să ne descopere cele mai ascunse secrete, să ne cunoască gândurile cele mai intime? Şi de ce nu ne pasă suficient pentru a lua măsuri?

Trăim într-o lume unde tot ceea ce spunem şi facem poate fi înregistrat, monitorizat, aşezat într-o bază de date, analizat, transmis serviciilor de securitate sau vândut unei companii specializate în marketing. Dacă urmăritorii noştri vor cu tot dinadinsul să vadă ce facem, ei pot îndrepta înspre noi un satelit de supraveghere, care ne poate detecta orice mişcare, zi sau noapte, în casă sau afară, pe furtună sau ceaţă. Ei pot, de asemenea, să se dispenseze de acest efort angajând o companie specializată în profiling. De la aceasta pot afla cine sunt vecinii noştri, ce sume avem în conturile noastre bancare, cât de mari sunt taxele

pe care le plătim (sau nu le plătim), de unde ne cumpărăm medicamentele, numele și adresele iubitelor / iubiților, informațiile din cazier, inclusiv numărul de la pantof. Ei știu toate acele mici secrete murdare pe care ai vrea să le păstrezi departe de ochii autorităților.

Ceea ce trebuie să acceptăm acum este faptul că am renunțat la intimitatea noastră în urmă cu mulți ani. Nu am luat decizia conștientă de a ne abandona dreptul la viața privată fără ca alți oameni să-și bage nasul unde nu le fierbe oala, ci pur și simplu s-a întâmplat. Pur și simplu am făcut cu mâna, în semn de „bun-rămas", tuturor măsurilor legislative pentru care au luptat înaintașii noștri, iar politicienii n-au avut habar ce se petrece. Nu am realizat că, în timp ce urmăritorii aflau tot ce voiau despre noi și transformau informațiile în profit, noi ne mulțumeam să ne uităm la televizor și să plecăm în vacanță. Așa că nu-mi pare deloc rău că am început ultimul capitol al acestei cărți reamintind cum Marea Britanie, până acum mai liberală și relaxată în comparație cu Statele Unite, s-a schimbat atât de mult.

Nu a durat mult pentru ca premierul britanic să fie copleșit de ceea ce el a numit „realitatatea dură" și „bunul-simț" după 11 septembrie 2001. În 1994, Tony Blair, liderul opoziției la acea vreme, a spus în Camera Comunelor: „Un cetățean nu poate fi privat de libertate prin decizia unui politician, ci numai prin decizia unei instanțe judecătorești". Cu toate acestea, ministrul de interne din guvernul lui Blair și-a acordat puteri excepționale, care îi permit să sechestreze la domiciliu orice persoană pe care o consideră o amenințare, fără ca decizia să treacă prin instanță. Reverendul Peter Selby, episcop de Worcester, a opinat, referindu-se la acest aspect: „Am rămas uimit când am văzut că guvernul a luat o măsură executivă într-un domeniu care îi aparține de drept puterii legislative". Explicația este faptul că, atunci când țara este atacată de un inamic, la scară națională, publicul are tendința să creadă că politicienii percep situația ca pe

o ocazie de a-şi extinde puterile. Dificultatea este să-i convingi pe politicieni, când faptul este consumat, să renunţe la puterile extinse şi să se reîntoarcă la vechiul sistem. Aşa cum se poate întâmpla şi cu libertăţile cetăţeneşti, cum sunt procesul cu juraţi şi prezumţia de nevinovăţie până la dovedirea vinovăţiei, dreptul nostru la viaţa privată nu mai înseamnă nimic acum.

Echelon, monstruosul sistem de colectare a datelor sponsorizat de serviciile de securitate din Marea Britanie şi Statele Unite şi sprijinit de naţiuni precum Canada şi Australia, poate să recepţioneze orice comunicaţie electronică între Orientul Mijlociu, Europa şi Statele Unite, în orice moment al oricărei zile. Asta reprezintă o reuşită tehnică remarcabilă, mai ales dacă te gândeşti că datele pe care le adună el sunt analizate, sortate, filtrate, rafinate electronic, până sunt reduse la materiale utilizabile, ce pot fi evaluate de nişte fiinţe umane. Teoretic, doar datele ce se referă la criteriile stricte formulate de serviciile de securitate pot fi obţinute astfel, dar cum putem şti asta cu siguranţă? Programul Echelon este revoluţionar şi nu a fost copiat nicăieri, în primul rând deoarece Statele Unite au resursele umane şi tehnice cerute, precum sateliţi militari de supraveghere foarte sofisticaţi şi staţii de monitorizare la sol cu personal calificat. Totuşi, francezii au acum propriul sistem – desigur, mai mic, dar, la fel ca Echelon, cu baza în spaţiu. Acesta este începutul unei curse. Când a început totul?

La o lună după atacul asupra World Trade Center („turnurile gemene“), administraţia Bush a adoptat „Actul Patriotic“ şi, în acest proces, a iniţiat atacul aferent asupra libertăţilor cetăţeneşti. Preşedintele Bush şi susţinătorii săi îşi percep naţiunea ca pe „Fortăreaţa America“, angajată într-un global „război împotriva terorii“, iar asta le oferă justificarea de care au nevoie pentru a ataca Afganistanul şi a mărşălui apoi prin Irak. Guvernul britanic, utilizând mulţimi de trafic de informaţii din întreaga lume, a strâns suspecţii de terorism şi i-a închis într-un gulag

de închisori de înaltă securitate. Când, într-un final, sistemul judiciar a spus guvernului că încalcă principiile constituţionale, toţi suspecţii au fost eliberaţi, înainte de a schimba Constituţia pentru a le permite să aresteze la domiciliu pe oricine ar vrea, fără punere sub acuzaţie şi proces.

Actualele dispute dintre partide în privinţa Constituţiei din Marea Britanie trebuie asociate cu atacurile prelungite asupra libertăţilor cetăţeneşti. Acestea includ nu doar un atac asupra principiilor procesului cu juraţi şi asupra prezumţiei de nevinovăţie, dar şi cererea ca fiecare să-şi dovedească existenţa plătind pentru propriul card de identitate. Toate acestea reprezintă tentative grave de a înclina balanţa puterii constituţionale în favoarea executivului. Sunt cereri care, chiar şi în Statele Unite, ar fi respinse imediat de Senat. Guvernul britanic a profitat de oportunitatea oferită de o majoritate parlamentară masivă pentru a corupe administraţia, chiar luând puterea din mâinile funcţionarilor de stat şi dându-le-o unor „aparatnici" sau „consilieri" nealeşi şi pornind la război în Irak, pe baza unor sfaturi neoficiale şi îndoielnice venite de la Procurorul General. Guvernul a ieşit basma curată după toate aceste abuzuri graţie majorităţii sale parlamentare, satisfacţiei oferite de o economie aparent sănătoasă, precum şi faptului că membrii electoratului destul de furioşi pentru a răsturna situaţia sunt prea puţini.

Cea mai semnificativă pierdere a libertăţii, care a trecut aproape neobservată de public, este nivelul de siguranţă dăunător şi constant care s-a strecurat în viaţa cotidiană a tuturor britanicilor. Electoratul observă foarte greu acest lucru, deoarece votanţii sunt mai preocupaţi de taxe şi impozite, guvernare locală şi centrală, imigraţie şi legislaţie. Însă va veni o zi când ei vor realiza că libertatea lor, odinioară cel mai valoros premiu, a dispărut pentru totdeauna.

Pierderea intimităţii nu a fost determinată doar de deciziile politicienilor, ea a rezultat şi din activităţi comerciale. E limpede

că în prezent există o uriaşă piaţă internaţională a informaţiilor, în care datele pot fi vândute sau schimbate cu parteneri din întreaga lume, în pofida asigurărilor enunţate în Legea protecţiei datelor şi în Legea libertăţii informaţiilor. În lumea „reţelei", companiile de marketing cu date trebuie să fie active în arena internaţională pentru a putea spera la succesul financiar. Marii jucători, care concurează unii împotriva celorlalţi şi folosesc poveştile noastre de viaţă ca materiale brute, sunt prea bogaţi şi puternici pentru ca politicienii pipernicţi să se opună eficient în mod legislativ.

Piaţa informaţiilor va înflori pentru că bazele de date sunt pretutindeni. Cea a Serviciului Naţional de Sănătate (NHS) conţine înregistrările medicale ale tuturor persoanelor din Marea Britanie. Pare trist că această conversie a tuturor datelor în formă computerizată anunţă sfârşitul acelor caiete-index vechi, conţinând notiţele medicilor de familie cu scrisul lor, prin tradiţie indescifrabil. Acele caiete cu mâzgălituri străvechi, pete de cafea şi hieroglife bizare, formule chimice complicate, detalii intime ale vieţii sexuale familiale, ale bolilor, accidentelor dureroase şi ale disfuncţiilor jenante genito-urinare au fost toate traduse cumva în limbajul computerelor. Eufemismele doctorilor, deseori scrise codat (de pildă „MDB" pentru „mort de beat") cu stiloul, pixul cu mină sau uneori creionul, au devenit desuete, acum că au fost transcrise într-o bază de date uriaşă, care va fi deschisă membrilor „acreditaţi" ai Serviciului Naţional de Sănătate.

De fapt, potenţialul de a se strecura erori va fi foarte mare şi, în consecinţă, riscul asupra sănătăţii – grav. Asta e ceea ce guvernul descrie drept „progres", dar cea mai îngrijorătoare este pierderea controlului asupra acestei nepreţuite resurse private. Simpla sa existenţă face ca personalul spitalului în care eşti primit pentru a te opera de prostată sau pentru a-ţi extrage măselele de minte va putea avea acces la istoria ta privată. Ca o consecinţă directă a creşterii industriei de colectare a datelor,

câțiva dintre cei privilegiați, care au acces la asemenea date confidențiale, vor primi stimulente serioase pentru a le vinde celor care pot profita cel mai mult de pe urma lor. Aici sunt inclusi nenumărați funcționari guvernamentali, administratori sanitari, consultanți, asistente, generaliști și paramedici, care vor dispune de acces facil la detaliile tale personale, chiar dacă asta este împotriva codului lor de bune practici.

Sănătatea va fi urmată curând și de educație. Înregistrările școlare de la autoritățile locale de sănătate vor fi adnotate și transferate într-o bază de date a Departamentului pentru Educație. Ce va include ea? Prezența la școală, pedepsele aplicate de profesori, notele pentru teme și rezultatele testelor? Opinii particulare ale unor dascăli ostili sau ale unor inspectori școlari? Vor fi aceste informații disponibile unor angajatori potențiali, care vor putea fi tentați să își bazeze judecățile pe opiniile profesorilor privind caracterul aplicantului, exprimate pe când acesta avea 12 ani? Cu toții ne schimbăm cu timpul. Ne maturizăm și ne dezvoltăm fizic, mental și emoțional. Creșterea și dezvoltarea sunt, desigur, influențate de experiențele trăite. Datele, așa cum reies din computer, sunt la fel de aride ca un schelet în deșert. Ele se bazează pe analize, deseori purtate automat de programul computerului, pentru a pune carne pe oasele goale. Este un fapt foarte îngrijorător că, în această formă brută, cantități imense de date sunt colectate fără permisiunea noastră sau fără vreo asigurare reală că ele nu vor cădea în mâinile unor persoane nepotrivite.

Nimic nu este mai adevărat decât maxima: „Informația înseamnă putere" și e evident că toți politicienii o acceptă fără a pune întrebări. Totuși, nu există o legislație relevantă care să ne protejeze împotriva utilizării nepotrivite a detaliilor noastre private. Legea protecției datelor nu face prea multe pentru a împiedica executivul să strângă și să păstreze informații despre viețile noastre. Oare protecția nu ar trebui să preceadă colectarea?

Îndoiala supărătoare pe care nu mi-o pot scoate din minte este: cât de sigure vor fi înregistrările mele de sănătate şi educaţie? Acest lucru e important pentru mine, deoarece nu vreau ca vreun broker de asigurări să afle că am avut febră reumatică în copilărie (ceea ce nu e adevărat) sau că am fost dat afară din şcoală pentru consum de droguri la 15 ani (ceea ce nu s-a întâmplat) sau că am avut o programare la clinica de boli venerice din Praed Street după ce am descoperit un furuncul urât la 18 ani (ceea ce poate fi adevărat). Însă mai rău decât potenţiala pierdere a intimităţii şi confidenţialităţii este înţelegerea faptului că baza de date a NHS-ului va fi una dintre cele mai complexe tentative din istorie de colectare a informaţiilor. Confidenţialitatea ei este vitală pentru toţi britanicii care pun preţ pe sanctitatea vieţii lor private. Totuşi, este responsabilitatea politicienilor şi a funcţionarilor publici să se asigure că nici o înregistrare medicală nu va cădea pe mâinile cui nu trebuie. Este o însărcinare fără speranţă de reuşită. Vor apărea tot felul de măsuri legislative şi promisiuni de pedepse grele pentru cei prinşi exploatând datele, însă industriile medicamentelor şi asigurărilor sunt multinaţionale, iar valoarea înregistrărilor medicale ale unei naţiuni este inestimabilă.

Acelaşi lucru este valabil şi în cazul educaţiei. De ce ar trebui ca opiniile personale şi foarte subiective din urmă cu ani buni ale unor persoane să fie accesibile azi fără permisiunea subiectului acestor afirmaţii? Mă tem că vor trece nu ani, ci luni până când poveştile vieţilor unui uriaş număr de cetăţeni britanici să ajungă pe mâna companiilor farmaceutice şi nu numai, care le pot achiziţiona. Când se va întâmpla acest lucru, mass-media, mereu nerăbdătoare să afle lucruri explicite şi personale despre public, îşi va pierde orice inhibiţie pe care ar putea-o avea privind întrebuinţarea abuzivă a datelor personale, dacă asta înseamnă că ar putea pune mâna pe detaliile privind dezintoxicarea sau comportamentul sexual din şcoală al vreunui star rock.

Bazele de date sunt produse ale tuturor departamentelor guvernamentale. Odată ce informaţiile de pe cardul de identitate sunt puse în comun şi verificate prin comparaţie cu alte date personale, incluzându-le pe cele de la Administraţia Financiară sau de la Departamentul Vamă şi Accize, cazierul şi baza de date tot mai mare a poliţiei, incluzând informaţii pentru recunoaşterea facială, baza de date a NHS-ului, uriaşa cantitate de cunoştinţe obţinute şi păstrate de pe smart carduri şi carduri de credit, înregistrările serviciului de Imigraţie, baza de date a Departamentului pentru Educaţie, Biroul Paşapoarte, permisele de conducere, conturile bancare şi de la biblioteci, Registrul Naţional de Naşteri, Căsătorii şi Decese – totul despre noi va fi ştiut. Asta e probabil mai mult decât ştim despre noi înşine.

Dacă publicul nu se va revolta împotriva întrebuinţării abuzive a informaţiilor care există deja în Marea Britanie şi în Statele Unite, baze de date enorme precum aceasta vor exista în mai puţin de 20 de ani. Banalul card de identitate va fi înlocuit cu o poveste a vieţii fiecăruia dintre noi, deţinută de stat. Datele vor fi inexacte, iar existenţa lor – profund neliberală. Totuşi, dosarele noastre cibernetice vor fi folosite pentru ca alţii să-şi formeze păreri despre noi şi ar putea deveni bazele unui stat poliţienesc. Statele Unite ne-au deschis drumul cu programul CAPPSII, menit a alcătui profilul întregii populaţii, pentru a identifica potenţialii terorişti pe listele de zbor ale avioanelor. Când ştii tot ce se poate şti despre o populaţie, iar informaţiile sunt conservate electronic, poţi începe să tragi concluzii pe baza tuturor cunoştinţelor acumulate. Referinţele încrucişate şi profilurile personale sunt deja practici comune. Nu e greu să ne imaginăm ce consecinţe groaznice ne aşteaptă dacă tehnologia aceasta va ajunge în mâinile unui stat foarte represiv.

Colectarea de date va continua şi serviciile de spionaj vor deveni tot mai puternice, adăugând sos la puternicul amestec de informaţii obţinute din înregistrări publice. MI5 şi MI6, cele

două braţe ale serviciilor secrete britanice, sunt însărcinate cu spionajul naţional, respectiv internaţional. Ambele servicii au cunoscut cel mai înalt nivel de alertă – „severă“ (generală) – din noiembrie 2003, când Al Qaeda a bombardat clădirea Consulatului Britanic din Istanbul, ucigându-i pe consulul general şi alte 25 de persoane. „Alertă severă“ înseamnă că un atac terorist este aşteptat şi pe sol britanic şi toate unităţile antiteroriste ale poliţiei, serviciilor secrete şi armatei, precum şi serviciile de urgenţă trebuie să fie mereu pregătite. MI5, serviciul de securitate internă, îşi are baza la patru sute de metri mai sus de Parlament pe Tamisa, la Thames House, lângă Galeriile Tate. Directorul General, Eliza Manningham-Buller, o spioană arţăgoasă şi carieristă, a fost nevoită să-şi asume vina pentru eşecurile spionajului la începuturile Războiului din Irak. Atât MI5, cât şi MI6 au fost supuse unor reforme impetuoase de când premierul Tony Blair a luat decizia de a intra în război, la 45 de minute după ce s-a afirmat că arme de distrugere în masă ar putea fi îndreptate asupra ţării. Serviciile de securitate au mai fost acuzate că l-au identificat pe doctorul David Kelly, expertul în arme chimice care şi-a luat viaţa când oamenii au fost scandalizaţi că dosarul care se presupunea că dă detalii despre resursele militare ale lui Saddam fusese de fapt falsificat. Era clar că trebuia făcut ceva după ce raportul Lordului Butler a afirmat că MI6 s-a înşelat privind armele deţinute de Saddam Hussein.

Reforma serviciilor de spionaj britanice a venit ca un anunţ tipic vag, ce înşira noi standarde de raportare şi verificare a erorilor, numirea unui nou şef al Analizei Informaţiilor care să supravegheze activitatea spionilor şi o „Cartă Whistleblower“ care le permite analiştilor îngrijoraţi că datele sunt contrafăcute să-şi dezvăluie îndoielile, fără să se teamă de repercusiuni ce le-ar putea periclita cariera. Agenţia a mai recrutat un „Consilier al personalului“, care va sta la dispoziţia analiştilor şi oficialilor nemulţumiţi de modul în care este folosit materialul. Mai mulţi

analiști au fost recrutați în MI6 și au fost adoptați „termeni-standard" pentru a descrie gradul de încredere al surselor secrete. Totuși, guvernul britanic a acceptat că dosarul pregătit ca parte a justificării de a intra în război cu Irakul era eronat și că viitoarele rapoarte precum acesta ar trebui să separe clar opiniile ministeriale de asertiunile Comitetului Unit de Informații.

Pare ciudat faptul că spionii noștri sunt monitorizați și îndrumați cu atâta atenție, iar comportamentul lor este analizat la sânge de stat, câtă vreme politicienii care au dat declarațiile privind amenințarea cu arme chimice de 45 de minute rămân mai presus de orice critică. În timp ce ministrul de la externe anunța reformele aduse serviciilor de spionaj și cum vor trebui ele să raporteze informațiile secrete de acum înainte, MI5, care are câteva sute de ofițeri implicați permanent în activități antiteroriste, recruta în Marea Britanie 1 000 de noi angajați. A mai fost stabilită o rețea de „birouri" locale, care să țină sub observație amenințările regionale. Numărul persoanelor implicate în spionarea britanicilor crește constant și, în timp ce activitățile lor sunt, desigur, ținute secrete, spionii au devenit mai vizibili și mai puternici în ultimii ani. În Londra, SO13, grupul antiterorist al poliției, angajează 900 de ofițeri pentru Divizia Specială (SO12) și Divizia Antitero (SO13), iar alți 1 500 au fost desfășurați în forțele regionale din West Mainlands, Manchester și Scoția. Unitatea de supraveghere de elită a armatei, Compania 14 de Spionaj, care s-a ocupat mulți ani de monitorizarea celulelor teroriste republicane și loialiste din Irlanda de Nord, a fost mutată pentru a sprijini regimentele militare specializate, precum SAS și SBC, în viitoarele lor operații din afara Marii Britanii. Unitatea e acum cunoscută ca Regimentul Special de Recunoaștere și staționează la Hereford (alături de SAS). Sarcina regimentului este de a oferi servicii de supraveghere secretă asupra organizațiilor teroriste înainte de intervenția forțelor speciale. Este unul dintre cele mai respectate regimente ale

forţelor armate britanice, iar probabila sa deplasare în Irak vine ca urmare a solicitării armatei americane. Deşi e o unitate mică, având mai puţin de 100 de bărbaţi şi femei, experienţa lor în supraveghere, căpătată pe străzile însângerate ale Belfastului, este considerată unică.

Creşterea numărului de cadre utilizate în activităţi de spionaj şi informaţii secrete pe teritoriul continental britanic s-a produs în mod evident ca răspuns la ceea ce se percepea a fi o ameninţare reală. Dar Eliza Manningham-Buller omite să spună cât de mare este această ameninţare. În particular, ea refuză să ofere cifre pentru că e de părere că, pe lângă un grup mic de terorişti devotaţi cauzei lor, pe teritoriul continental există un număr nedefinit de simpatizanţi care ar putea sau nu să ofere sprijin, dar care s-ar face că nu ştiu nimic despre activităţile teroriste ale celorlalţi dacă ar fi întrebaţi. O sursă neoficială MI5 a estimat că până la 3 000 de tineri musulmani britanici au participat la taberele de antrenament ale Al Qaeda înainte ca acestea să fie închise în 2002. Lordul Hoffman, responsabilul juridic care a inspectat suspecţii deţinuţi fără proces la Belmarsh, crede că cifra se apropie de 1 000.

Ocazional, apar diverse informaţii oferite de serviciile secrete, cum ar fi faptul că Centrul Unit de Analiză a Terorismului de la Thames House a primit 60 000 de informaţii despre un atac iminent şi că atacul, când şi dacă se va întâmpla, va fi un atac convenţional sinucigaş cu bombă în timpul unui moment important, cum ar fi alegerile generale sau începutul unei noi sesiunii a Parlamentului. Dar stă în firea Al Qaeda să lovească în momente neaşteptate ţinte neprevăzute. Osama Bin Laden este un strateg strălucit, iar timpul este în mâinile sale. La un summit internaţional despre „Democraţie, terorism şi securitate", ţinut la Madrid în 2005, s-a insistat asupra ideii că este vital să se lupte împotriva terorismului fără a compromite libertatea. Una dintre concluzii era că agenţiile care aplică legea au nevoie

de puteri pentru a-şi face treaba, dar că nu trebuie să sacrifice niciodată principiile pe care sunt menite să le apere.

Problema este că serviciile secrete nu au acceptat niciodată că trebuie să joace un rol în procesul juridic şi multe din lucrurile pe care le fac rămân neînregistrate. După părerea agentului secret profesionist, suspiciunea este suficientă pentru a închide pe cineva. Serviciile secrete sunt întotdeauna refractare la oferirea de „probe“ dacă în felul acesta le e compromisă sursa. Activităţile lor nu trebuie expuse niciodată analizei şi examinării minuţioase a vreunui tribunal regal, spun ei. Interceptarea apelurilor telefonice a fost ilegală în Marea Britanie până la mijlocul anilor 1980. Puteai să faci înregistrări dacă făceai o cerere la Ministerul de Interne şi ţi se aproba. Pentru a putea fi efectuată, interceptarea trebuia să facă parte dintr-o investigaţie privind activităţi criminale deosebite sau să aibă de a face cu apărarea securităţii statului, şi asta numai dacă informaţia nu putea fi obţinută în alt mod. Dar apoi legislaţia s-a relaxat. Imediat au apărut poveşti despre comportamentul incorect al agenţilor MI5, care, pe lângă spionarea ambasadelor şi consulatelor ţărilor de dincolo de Cortina de Fier, au început să se amestece şi în treburile sindicatelor şi organizaţiilor cum ar Campania pentru Dezarmare Nucleară (CDN). Aceasta nu a avut nimic de a face cu un proces legal. MI5 nu a încercat să construiască un caz legal, ci doar aduna informaţii secrete şi construia o imagine pentru a arăta că „ştia ce se întâmplă“. Nu a existat nici cea mai vagă sugestie că vreuna dintre conversaţiile înregistrate de MI5 va fi folosită în vreun proces.

O hotărâre a Curţii Europene a Drepturilor Omului a obligat guvernul să promulge în 1985 Legea interceptării comunicaţiilor, care stabilea condiţiile generale de desfăşurare a interceptărilor. Actul păcătuia însă prin aceea că excludea total tribunalele din această chestiune. Printre altele, legea stabilea ca pe durata procesului să fie interzise prezentarea dovezilor sau întrebările

care ar fi putut indica existenţa unei interceptări, fie aceasta cu sau fără mandat. Pasajul în cauză a fost introdus deoarece serviciile secrete se temeau că în timpul proceselor s-ar fi putut face referire la activitările lor ilegale de interceptare a convorbirilor din trecut, care între timp deveniseră legale, şi că ar putea trage ponoasele de pe urma ilegalităţilor pe care le comiteau încă. Nici măcar în cazurile de siguranţă naţională nu sunt permise dovezile provenite din interceptări. Reprezentanţii sistemului judiciar resping aceste măsuri speciale, în primul rând deoarece astfel ofiţerii şi spionii serviciilor secrete primesc imunitate în faţa justiţiei. Judecătorii nu privesc cu ochi buni nici faptul că guvernul a susţinut această decizie. Poliţia, procuratura, grupul de presiune Liberty, Comitetul parlamentar reunit al drepturilor omului, toate aceste organisme au catalogat restricţiile ca fiind „ridicole“. George Churchill-Coleman, fost şef al unităţii antiteroriste a Scotland Yard, a atras atenţia asupra faptului că Marea Britanie devine din ce în ce mult un stat poliţienesc: „Refuzul serviciilor secrete de a consimţi ca dovezile obţinute din interceptări să poată fi utilizate în sălile de judecată, precum şi ajutorul de care s-au bucurat din partea stăpânilor lor politici sunt dovezi străvezii ale faptului că este dorinţa comună a unor factori de decizie importanţi din sistemul nostru politic şi de siguranţă naţională să devenim în scurt timp un stat poliţienesc“.

Serviciile secrete britanice răspund doar în faţa unui atotputernic director, care a dovedit de nenumărate ori că nu are scrupule în a scormoni în vieţile noastre pentru a-şi atinge propriile scopuri. Pe măsură ce MI5 şi MI6, precum şi bazele de date naţionale se dezvoltă, scenariile apocaliptice privind atentate teroriste viitoare se vor înmulţi, până când, în ciuda puţinătăţii dovezilor, teama pentru propria noastră siguranţă va învinge nevoia de intimitate. Militarii în rezervă rareori văd într-un card de identitate un atentat la drepturile civile, deoarece au purtat un card de acces de-a lungul întregii lor cariere.

Mulţi civili, de toate condiţiile şi cu pregătiri din cele mai diferite, nu consideră că au de ce să se teamă de o bucată dreptunghiulară de plastic. Desigur, nu cardul de identitate în sine pune în pericol drepturile cetăţeneşti, ci proliferarea camerelor de supraveghere şi a bazelor de date internaţionale, coroborate cu activitatea acerbă şi în forţă a poliţiei şi a serviciilor secrete, care se bucură în prezent de toate resursele de care ar putea avea nevoie în lupta cu terorismul. Luaţi în calcul de asemenea voinţa politică pentru ca nimeni din Marea Britanie şi America să nu fie lăsat în plata Domnului, precum şi viteza ameţitoare cu care se dezvoltă noile tehnologii, şi veţi recunoaşte semnele rău-prevestitoare.

Centrala de interceptare americană de la Menwith Hill şi complexul destinat spionajului electronic de la GCHQ din Cheltenham, Marea Britanie, pot monitoriza toate telefoanele şi e-mailurile transmise din sau tranzitând arhipelagul britanic. Şi, dacă o pot face, fiţi siguri că nu o să se gândească de două ori. Desigur, personalul este insuficient pentru a monitoriza absolut toate comunicaţiile; oricum, cea mai mare parte dintre acestea nu valorează nimic pentru părţile interesate, fie că vorbim de fisc, de poliţie sau de lanţul de retail Tesco. Prin intermediul unui soft se pot selecta, însă, materialele relevante; cuvinte şi fraze-cheie, surse şi destinaţii suspecte, limbi străine folosite, toate pot fi identificate şi aduse în atenţia serviciilor secrete. Programele şi viteza de calcul sunt îmbunătăţite constant, deoarece nevoia de informaţii creşte de la o zi la alta.

Conştientă de fluxul de populaţie din Europa şi Orientul Apropiat, CIA se foloseşte permanent de resursele impresionante de calcul de care dispune pentru a analiza şi a aduce la zi lista persoanelor considerate ca fiind „suspecte". Această bază de date conţine 6 000 de nume şi se alcătuieşte prin coroborarea mai multor criterii, cum ar fi tipare de mişcare (destinaţiile de călătorie şi frecvenţa vizitelor), locul naşterii, ba chiar numele şi

adresele rudelor. Această listă de nume este împărtăşită cu state partenere. Monitorizarea se realizează în Statele Unite, în Marea Britanie şi în Europa continentală, iar serviciile secrete britanice sunt îmboldite permanent să furnizeze agenţiilor americane orice aspect semnificativ privind activitatea persoanelor de pe listă.

George Friedman, fondator al reputatei Stratfor, agenţie independentă de informaţii cu sediul în Statele Unite, consideră că problema serviciilor secrete britanice şi americane este tendinţa lor de a se bizui pe „surse şi informaţii, mai degrabă decât pe o cunoaştere reală, din interior, a problemelor". Sursele secrete şi bazele de date pot fi utilizate pentru a susţine o analiză; nu şi o idee, însă. Nimeni nu poate lua o hotărâre fără să se bazeze pe informaţiile furnizate de surse sau de baze de date. Când cineva o face şi dă greş, atunci e vai de pielea lui. CIA şi MI5 sunt cum nu se poate mai minuţioase în chestiunile de mică importanţă, dar au tendinţa să se înşele cu totul în ceea ce priveşte problemele importante. Sediul CIA din Langley, Virginia, geme de ofiţeri care susţin că au prezis atacul asupra turnurilor gemene de la 11 septembrie. Ce-i drept, anterior atentatului, au avut loc exerciţii în care terorişti arabi intrau cu avioane de linie în World Trade Center. Era doar unul dintre sutele de scenarii posibile şi nu a fost luat în serios. Teoria CIA conform căreia Al Qaeda era răspândită la nivel global şi avea drept ţintă Statele Unite se baza pe viziune, nu pe dovezi ori pe informaţii strânse de la surse. Când agenţii CIA au aflat de la surse că agenţii Al Qaeda aveau bază într-un oraş european, această informaţie a fost introdusă într-o analiză. Câteva zile după 9/11, CIA nu avea nici cea mai mică idee dacă Statele Unite se aflau în război cu Vestul sau aveau de-a face cu o şleahtă de infractori.

Viziunea apare rar în serviciile secrete; când apare, la Langley nu e bine-venită şi la Thames House e hulită de-a dreptul. Rezultatul e cel enunţat anterior: CIA şi MI6 se pricep la

nimicuri, dar le lipseşte imaginea de ansamblu. Ofiţerii şi conducerea se bizuie doar pe informaţiile şi analizele obţinute de la surse umane şi pe aportul bazelor de date secrete pentru a-şi întemeia hotărârile, conştienţi permanent de ceea ce stăpânii lor din sfera politicului ar dori să citească în informările pe care le primesc, venind permanent în întâmpinarea dorinţelor lor.

Următorii zece ani vor fi caracterizaţi fie de o sporire exponenţială a cantităţii de informaţii personale strânse de către stat, fie de o revoltă spontană împotriva încălcării dreptului la viaţa privată. Combatanţii acestei lupte vor fi, pe de-o parte, publicul şi organizaţiile nonguvernamentale, şi politicienii şi marile corporaţii, care văd în oameni nişte instrumente de marketing, bune doar să muncească şi să voteze, de cealaltă parte. Nu există interes public pe care această ultimă perspectivă să-l servească. Nu există onoare în acest punct de vedere. Mama mea, văduvă la peste 90 de ani, trăia într-un azil de bătrâni şi, totuşi, primea regulat scrisori de la marile trusturi financiare. Nu o deranja, deoarece simţea că astfel stabileşte o punte de comunicare cu lumea exterioară. Nimeni nu le cerea, şi totuşi scrisorile continuau să vină, cu scopul vădit de a profita de pe urma vulnerabilităţii ei. Mai vorbeam din când în când cu ea, pentru a-i lua apoi scrisorile şi a le arde. În cele din urmă, corespondenţa nesolicitată a fost interzisă la azilul unde era mama internată când un bătrân şi-a pierdut averea după ce a răspuns la o astfel de scrisoare. Informaţia înseamnă putere, dar impune responsabilitate. Avem nevoie de o legislaţie adecvată pentru a ne asigura de utilizarea înţeleaptă a informaţiei, pentru a preveni exploatarea celor vulnerabili.

De ce nu am face ceva ACUM pentru a opri această încălcare a drepturilor noastre civile? Se impune revizuirea de urgenţă a legii privind viaţa privată. Când dezbaterea privind cardul de identitate va reveni în Parlament, s-ar putea să fie ultima noastră şansă să scăpăm de pacostea asta, o dată pentru totdeauna.

Şi, dacă tot ne vom fi apucat, am putea băga şi guvernul, şi corporaţiile în curăţenie generală, mai cu seamă colţurile murdare unde sunt strânse secretele noastre pentru a fi introduse în computere, acelea în care se pregăteşte folosirea lor împotriva noastră. Un prim pas ar putea fi desfiinţarea monopolurilor de stat şi comerciale de colectare a informaţiilor despre alegători, aflate deocamdată în afara oricărui control. Avem nevoie, mai ales, de o legislaţie nouă, care să instituie dreptul nostru la viaţa privată, care să ne lase să ne trăim viaţa, fără imixtiunea statului şi a marilor companii. Abia atunci libertăţile despre care credeam că ni se cuvin de la naştere, dar de care suntem privaţi încet-încet, vor fi instaurate o dată pentru totdeauna.

Bibliografie

BALL, KIRSTIE S. şi WEBSTER, FRANK, *The Intensification of Surveillance: Crime, Terrorism and Warfare in the Information Age,* Pluto Press Ltd, 2003

BERKOWITZ, BRUCE D. şi GOODMAN, ALLEN E., *Best Truth: Intelligence in the Information Age,* Yale University Press, 2002

BRIN, DAVID G., *The Transparent Society: Will Technology Force Us to Choose Between Privacy and Freedom?,* Perseus Books, 1999

CORBIN, JANE, *The Base: Al Qaeda and the Changing Face of Global Terror,* Pocket Books, 2003

DEARNLEY, JAMES şi JOHN FEATHER, *The Wired World: An Introduction to the Theory and Practice of the Information Society,* Library Association, 2001

DENNING, DOROTHY E., *Information Warfare and Security,* Addison Wesley, 1999

DRAKOS, PETER şi JOHN BRAITHWAITE, *Information Feudalism: Who Oums the Knowledge Economy,* Earthscan Publications, 2002

FEATHER, JOHN, *The Information Society: A Study of Continuity and Change,* Facet Publishing, 2004

FRANK, MITCH, *Understanding September 11th: Answering Questions about the Attack on America,* Viking Books, 2002

GARFINKEL, SIMPSON, *Database Nation: The Death of Privacy in the 21st Century,* O'Reilly UK, 2001

GARLAND, DAVID, *The Culture of Control: Crime and Social Order in Contemporary Society,* Oxford University Press, 2002

LESSIG, LAWRENCE, *Free Culture: How Big Media Uses Technology and the Law to Lock Down Culture and Control Creativity,* Penguin USA, 2004

LEVIN, THOMAS Y., *CTRL (Space): Rhetorics of Surveillance from Bentham to Big Brother,* MIT Press, 2002

LYON, DAVID, *Surveillance after September 11,* Blackwell Publishing, 2003

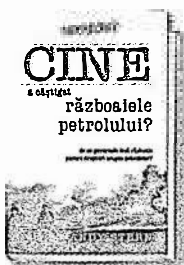
LYON, DAVID, *Surveillance as Social Sorting: Privacy, Risk, and Automated Discrimination,* Routledge, 2002
LYON, DAVID, *Surveillance Society: Monitoring Everyday Life,* Open University Press, 2001
MACKEY, CHRIS şi GREG MILLER, *The Interrogator's War: Inside the Secret War Against Al Qaeda,* John Murray, 2004
MCGRATH, JOHN, *Loving Big Brother: Surveillance Culture and Performance Space,* Routledge, 2004
O'HARROW, ROBERT, *No Place to Hide,* Free Press, 2005
PARKER, JOHN, *Total Surveillance: Investigating the Big Brother World of E-spies, Evesdroppers and CCTV,* Piatkus, 2001
RAI, MILAN, *Regime Unchanged: Why the War in Iraq Changed Nothing,* Pluto Press, 2003
RAMESH, RANDEEP, *The War We Could Not Stop: The Real Story of the Battle for Iraq,* Faber and Faber, 2003
RIDDELL, PETER, *Hug Them Close: Blair, Clinton, Bush and the „Special Relationship",* Politicos, 2004
RIDDELL, PETER, *The Hidden Hand: Britain, America and Cold War Secret Intelligence,* John Murray, 2002
RITTER, SCOTT, *War on Iraq: What Team Bush Doesn't Want You to Know,* Profile Books, 2002
SCHULSKY, ABRAM M. şi GARY J. SCHMITT (ed. Gary J. Schmitt), *Silent Warfare: Understanding the World of Intelligence,* Brassey's US, 2002
SIFRY, MICAH L. şi CHRISTOPHER CERF (eds.), *The Iraq War Reader: History, Documents, Opinions,* Touchstone Books, 2003
SILVERS, ROBERT B. şi BARBARA EPSTEIN, *Striking Terror: America's New War,* New York Review of Books, 2002
SIMPSON, JOHN, *The Wars Against Saddam: Taking the Hard Road to Baghdad,* Macmillan, 2003
STAUBER, JOHN, *Weapons of Mass Deception,* Constable and Robinson, 2003
STOTHARD, PETER, *30 Days: A Month at the Heart of Blair's War,* HarperCollins, 2003
TODD, PAUL şi JONATHAN BLOCH, *Global Intelligence: The World's Secret Services Today,* Zed Books, 2003
WEBSTER, FRANK, *Theories of the Information Society,* Routledge, 2002
WEBSTER, FRANK şi ENSIO PUOSKARI, *The Information Society Reader,* Routledge, 2003
WOODWARD, *Plan of Attack,* Simon and Schuster, 2004

TITLURILE SERIEI

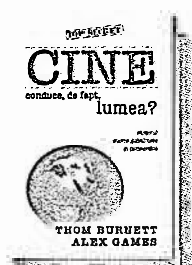
TOP SECRET



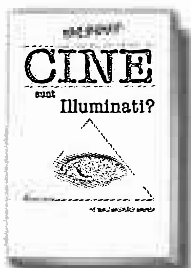
Cine a câştigat, de fapt, cursa spaţială?



Cine a câştigat războaiele petrolului?



Cine conduce, de fapt, lumea?



Cine sunt Illuminati?



Ce este Opus Dei?

TOP SECRET

O serie de cărţi care examinează, pe baza unei documentaţii ample şi a unei analize de mare fineţe, cele mai interesante momente ale istoriei moderne, contemporane şi recente, evenimente care au marcat, uneori decisiv, cursul civilizaţiei umane în ultima sută de ani.

La ora actuală, în epoca tehnologiei sofisticate, guvernele și entitățile desemnate de ele au capacitatea de a-i urmări pe cetățeni nu numai pe stradă (camerele de luat vederi se află peste tot în Marea Britanie), ci și în casele lor particulare (lăsăm o amprentă ori de câte ori folosim Internetul). Guvernele afirmă că această supraveghere are loc pentru siguranța noastră, dar amenințarea de tip „Big Brother", așa cum a fost ea descrisă de George Orwell, devine tot mai mult realitate.

Cartea analizează, pe parcursul celor 11 capitole ale sale, toate modalitățile de supraveghere la care sunt supuși cetățenii, cu sau fără știrea acestora, modalități de multe ori ilegale, dar bazate pe principiul că informația și cunoașterea înseamnă putere. Întrebarea finală este în ce măsură se mai poate vorbi despre libertate personală într-o lume în care statul supraveghează orice mișcare a cetățenilor săi.



rao international publishing company

ISBN 978-973-54-0069-9



www.rao.ro
www.raobooks.com